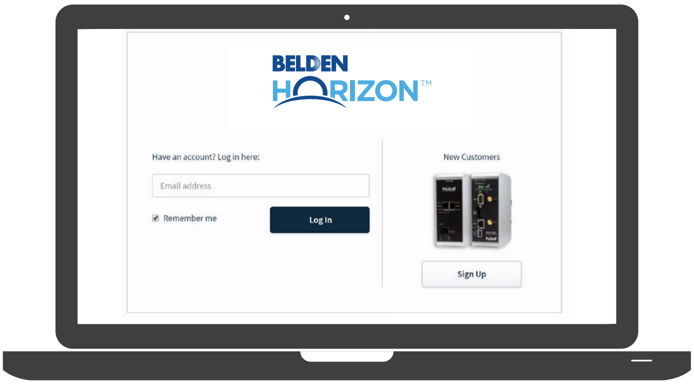
Belden Horizon™

Powerful Console Enabling Secure Remote Connectivity and Edge Orchestration

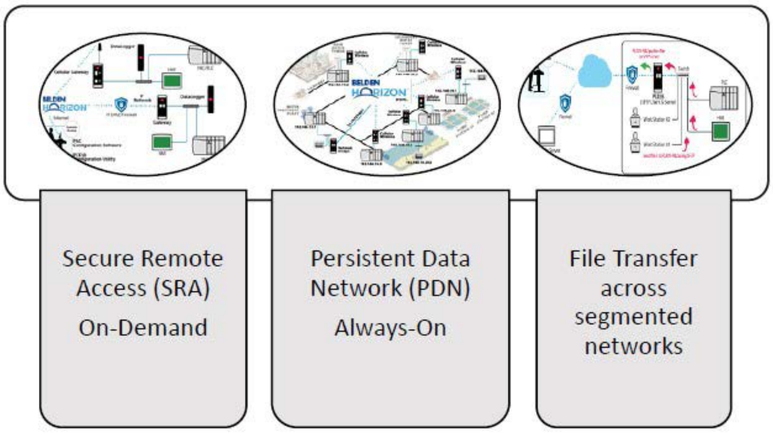
TECHNICAL OVERVIEW

The purpose of this document is to provide a technical overview of how Belden Horizon works and the different security features. This document should be used in conjunction with the **Belden Horizon datasheet**. The intended audience is OT (Operational Technology) and IT (Information Technology) professionals. This document explains how the platform's secure remote connectivity capability works at a high level.



Belden Horizon™ – Simple, Secure, and Managed

Belden Horizon is an industrial remote connectivity and edge orchestration software platform. It is a cloud-native service that is easy to use, secure, and optimized for highly reliable performance. The platform has been engineered specifically for mission-critical industrial process/plant/machine uptime. Belden Horizon supports multiple applications.


Secure Remote Access (SRA)
On-Demand
Persistent Data Network (PDN)
Always-On
File Transfer across segmented networks

- **Secure Remote Access (SRA) or Secure Machine Access (SMA).** SRA allows an automation technician or an authorized service provider (like a systems integrator or a machine builder) to connect to a specific machine to troubleshoot or perform routine maintenance. SRA, if implemented correctly, can help reduce downtime, and provide improved first incident response and easier access to outside expertise. Belden Horizon's SRA application will enable you to have a positive impact on productivity and profitability without needlessly exposing other parts of your network.
- **Persistent Data Network (PDN).** PDN establishes a permanent connection between geographically dispersed locations for a SCADA-type network, like monitoring a municipal water utility or a gas distribution network. PDN is simple, secure, and managed, allowing users to focus on their primary objective – delivering on their continuous service.
- File transfer. Receive files from devices on the OT network (like a PLC) and then transfer the files to an IT network for backup without creating a connection between the OT and IT network.

The Main Components of Belden Horizon's Remote Connectivity

- There are two main components for applications supported by this platform - subscriptions and a gateway to enable connectivity to your application.
- Belden Horizon can be accessed via any web browser.
- There are two gateways – a **wired gateway (PLX35-NB2)** and a **cellular gateway (ICX35-HWC-A, ICX35-HWC-E)**.
- For applications that require connectivity to a cloud instance, a Virtual Node (VN-PDN) is also available.

Download on the App Store

Belden Horizon is mobile-ready with dedicated apps available for download on the iOS platform.

Belden Horizon uses Containers to deploy Quickly and Reliably

Belden Horizon leverages the power of cloud computing. It uses well-established standard technologies to provide enhanced security and ease of use, but makes it invisible to the end user. The platform runs on Kubernetes® and uses containers for high availability and reliability. Kubernetes is an open-source platform that is secure, reliable, and cloud-agnostic. It is the foundation for Belden Horizon's remote connectivity application.

This containerized architecture allows for Belden Horizon to be deployed quickly and reliably. Multiple containers mean there is no single point of failure. All services are hosted across multiple regions in AWS (Amazon Web Services). AWS uses Elastic Compute Cloud (EC2) as virtual servers. Belden Horizon is hosted on a variety of EC2s, which are not used for anything other than platform-related services.

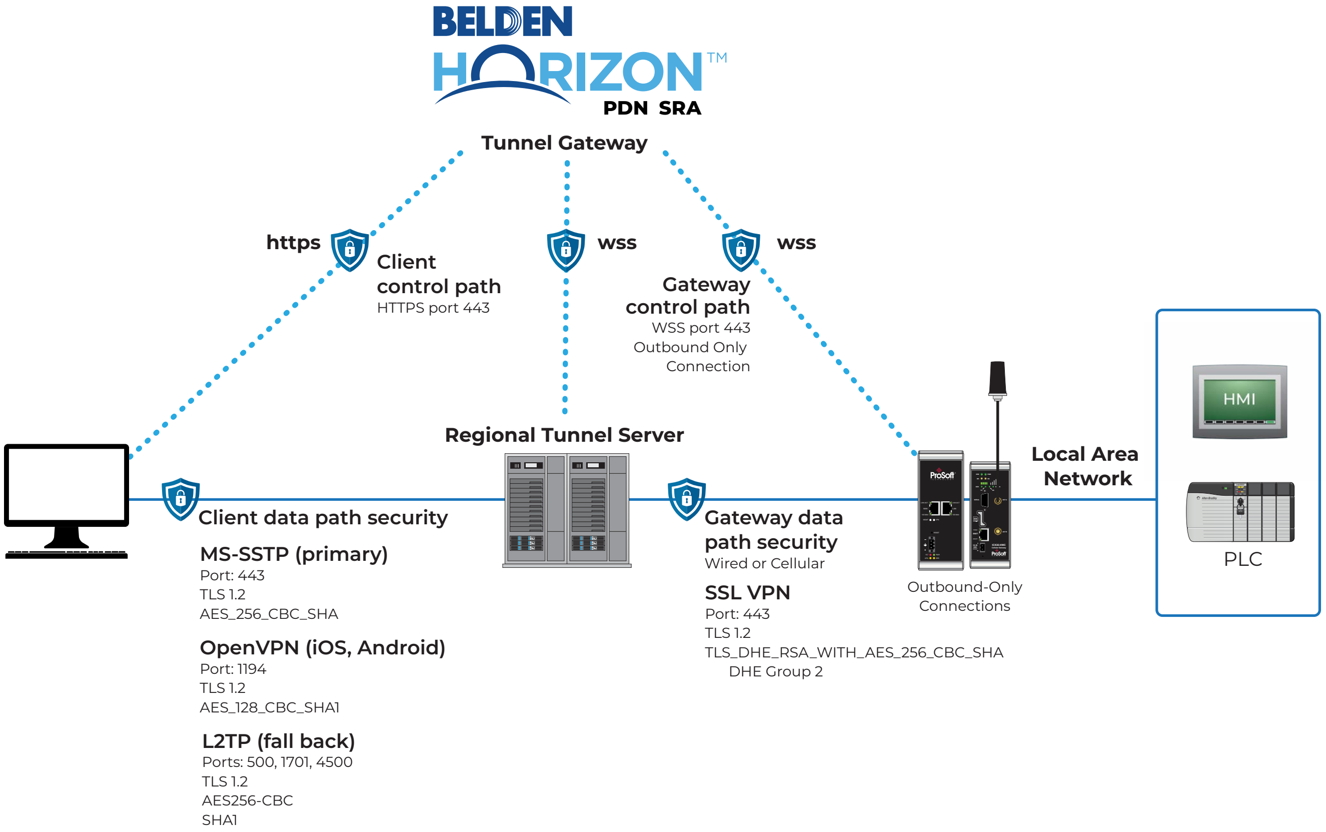
kubernetes

Belden Horizon uses containers for quick and reliable deployment

The CAIQ (Consensus Assessment Initiative Questionnaire) v3.1 framework governs our security policies while IEC62443 principles govern our design and development policies and ISO27001 principles govern our information security policies.

The following diagram is a high-level overview of Belden Horizon's connectivity architecture with the cipher suites information.

The remote user uses secure http (https) to form the connection to the cloud. The gateway uses secure web sockets (WSS) to form the connection to the cloud. The connection is completed after the keys are verified. The platform uses a native protocol on top of WSS. The Belden Horizon data plane uses a combination of VPN protocols MS-SSTP, SSL-VPN, L2TP, and OpenVPN (only for mobile devices).



The remote user uses secure http (https) to form the connection to the cloud. The gateway uses secure web sockets (WSS) to form the connection to the cloud. The connection is completed after the keys are verified. The platform uses a native protocol on top of WSS. The Belden Horizon data plane uses a combination of VPN protocols MS-SSTP, SSL-VPN, L2TP, and OpenVPN (only for mobile devices).

Belden Horizon is Easy To Use

As a productivity tool, it is designed to help the user accomplish their primary task, be it getting the machine back online as quickly as possible or ensuring the city's utilities are functioning correctly.

Belden Horizon is easy to use because:

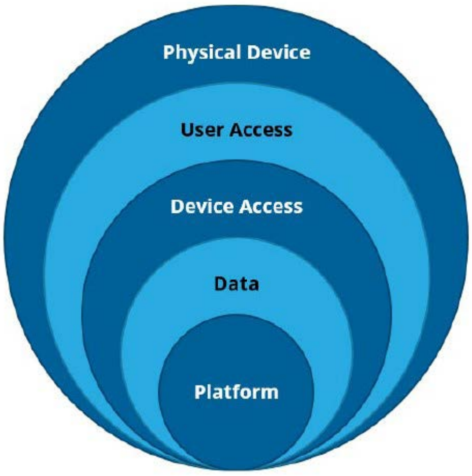
- It is cloud-native – no software to install or maintain – simply connect to the platform at **belden.io.**
- It is platform-agnostic – works with any browser and on any platform or device. There are dedicated apps for mobile devices.
- Anytime, anywhere remote access to all of your sites
- Remotely see device and network diagnostics and activity log records of login/logout events and tunneling events
- Remotely authorize temporary access to external contractors for quick problem resolution
- No in-house networking or security expertise is required to deploy a network with >99% uptime - everything is managed by Belden Horizon.

Belden Horizon is Secure

The platform is a tool designed for OT professionals to help improve productivity when troubleshooting machines or a process, or to connect remote assets to a central SCADA system. Given the convergence of OT and IT networks, a secure remote connectivity solution is vital. The platform uses a multilayered, defense-in-depth approach (aligned with IEC62443) to security to ensure your system is always protected.

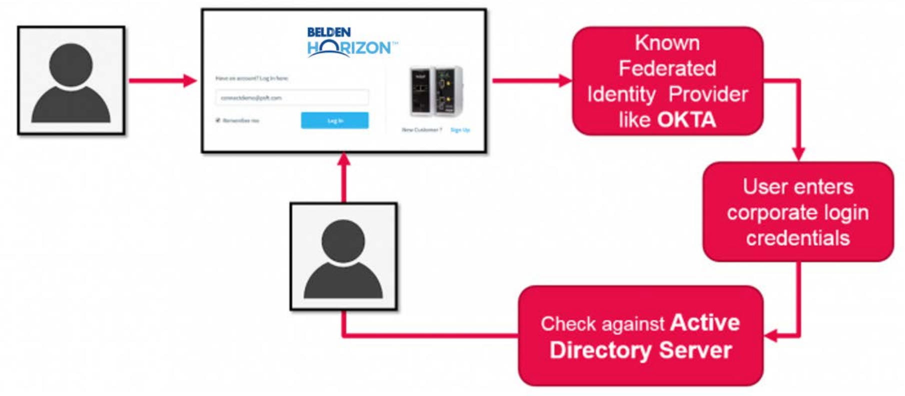
There are five layers of security. Let's look at each one of these layers in more detail.

The outmost layer that needs to be secured is the **Physical Device**. Device security includes digitally signed firmware and support for outbound connections only on ProSoft's two remote access gateways – ICX35 and PLX35.



Belden Horizon deploys Defense-In-Depth – a multilayered approach to security.

Digitally signed firmware means that the firmware file is verified to be from the right source before the device (or gateway) will accept the file. Any firmware change is logged and can be exported for future forensic use. The firmware itself is Linux OS-based and is field upgradeable. The firmware is a combination of off-the-shelf open source software and other applications to manage the device. These run continuously on the gateway. Compared to PC-based or server-based remote access solutions, device-based remote access offers a much smaller attack surface and is designed specifically for machine remote access.


BELDEN HORIZON
Log In
Known Federated Identity Provider like OKTA
User enters corporate login credentials
Check against Active Directory Server

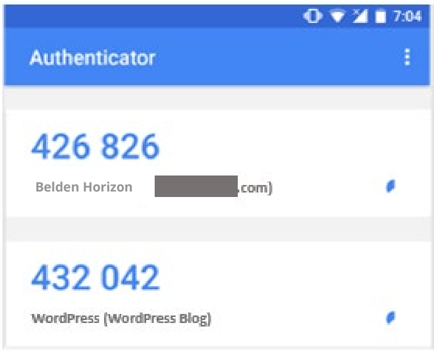
The gateway only initiates outbound connections. By default, the gateway only accepts HTTP and HTTPS connection requests. These can be disabled if one only wants to configure the gateway through Belden Horizon. With correctly implemented DMZs (de-militarized zones), all inbound connections can be blocked. To use the gateway in the platform, we don't need to accept any inbound connections.

The next layer to be secured is **user access** - an important security layer. This layer determines how the user accesses the platform. Since IT and OT networks are converged, Belden Horizon supports Active Directory via Single Sign-On (SAML 2.0) as one of the login types. Single Sign-On, or SSO, allows IT to add Belden Horizon access to an IT-controlled user list. This way, if IT revokes a user's login credentials, then that user's access to Belden Horizon will automatically be revoked. For OT professionals, support for SSO means that they don't need to create, save, and remember multiple usernames and passwords. All login activity is recorded in the activity log.

To further fortify user access, the platform allows users to set their own password policy. This allows users to determine password complexity requirements and mandatory rotation periods that may be in line with existing policies. Configurable policy rules include enforcing minimum password length, password expiration period, requiring alpha-numeric characters, and much more.

Additionally, the platform incorporates token-based two-factor authentication (2FA). This requires the user to register their Belden Horizon username on a standard authentication app (like the Google Authenticator) for a two-step verification of the user's login credentials before accessing the platform.

Belden Horizon does support standard login whereby a user must enter the username and password (simple or complex) with two-factor authentication by email. All login activity is recorded in the activity log.


Authenticator

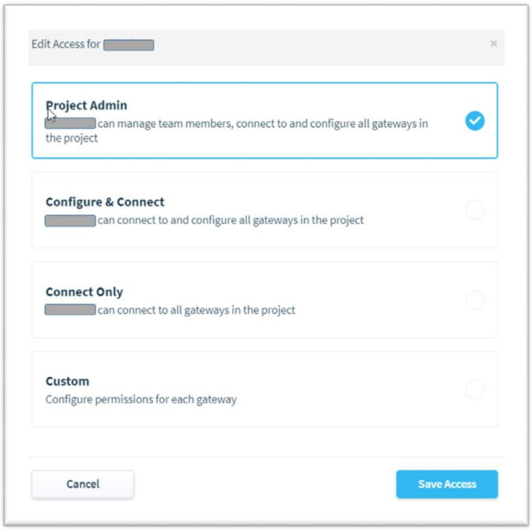
426 826
Belden Horizon [redacted].com)

432 042
WordPress (WordPress Blog)

Token-based 2FA

Next, **device access** must be secure. This layer deals with users initiating a secure connection to the gateway once they are logged in to Belden Horizon. Logging into the platform does not allow the user to access the end device like a PLC (programmable logic controller) or a HMI (human machine interface).

A user with administrative access can configure users to access specific projects and/or specific gateways in Belden Horizon. For example, a machine builder may want certain technicians to access projects specific to the customer they are servicing. Another example is an HVAC company with hundreds of gateways at different customer sites – they will want to only give their technicians access to gateways at customer sites for which they are responsible.



Edit Access for [redacted]

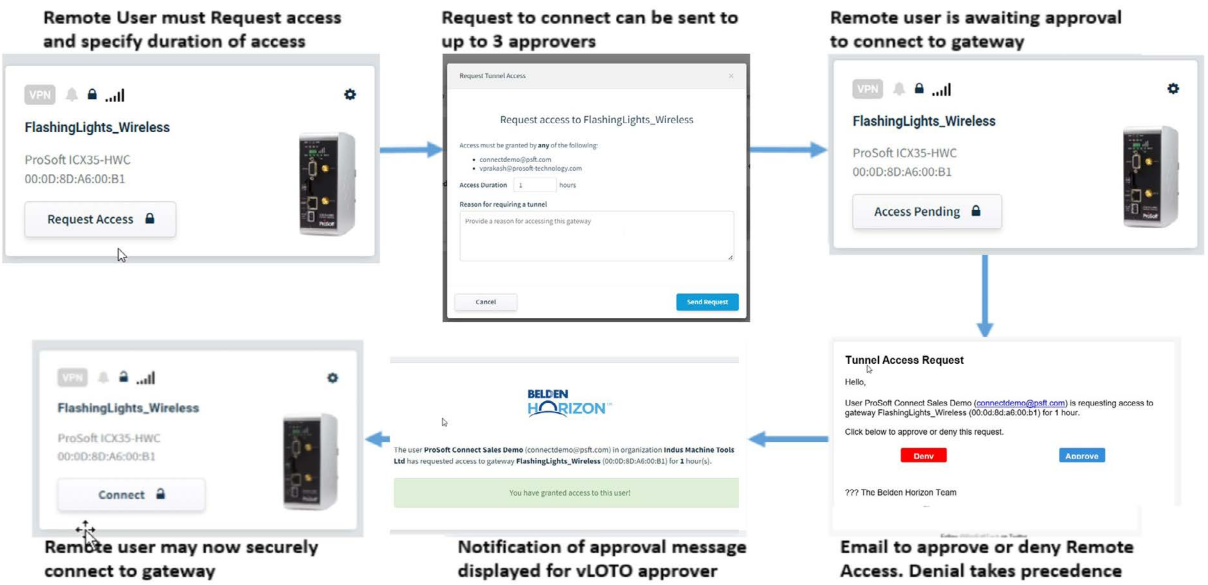
Project Admin
[redacted] can manage team members, connect to and configure all gateways in the project ●

Configure & Connect
[redacted] can connect to and configure all gateways in the project ○

Connect Only
[redacted] can connect to all gateways in the project ○

Custom
Configure permissions for each gateway ○

Virtual Lockout-Tagout (vLOTO™) is a unique feature of Belden Horizon and a powerful part of the device access security layer. vLOTO allows plant personnel to directly approve or deny every remote access request. Multiple personnel can be configured as approvers. vLOTO™ greatly enhances the security of the remote access solution as it allows the end user to be part of the remote connectivity process. vLOTO allows an authorized approver to enable or deny remote access at any time – even if a remote user is connected.



Remote User must Request access and specify duration of access

FlashingLights_Wireless
ProSoft ICX35-HWC
00:0D:8D:A6:00:B1

Request to connect can be sent to up to 3 approvers

Request Tunnel Access

Request access to FlashingLights_Wireless

Access must be granted by **any** of the following:

- connectdemo@psft.com
- vprakash@prosoft-technology.com

Access Duration 1 hours

Reason for requiring a tunnel

Provide a reason for accessing this gateway

Remote user is awaiting approval to connect to gateway

FlashingLights_Wireless
ProSoft ICX35-HWC
00:0D:8D:A6:00:B1

Tunnel Access Request

Hello,

User ProSoft Connect Sales Demo (connectdemo@psft.com) is requesting access to gateway FlashingLights_Wireless (00:0d:8d:a6:00:b1) for 1 hour.

Click below to approve or deny this request.

??? The Belden Horizon Team

Email to approve or deny Remote Access. Denial takes precedence

The user **ProSoft Connect Sales Demo** (connectdemo@psft.com) in organization **Indus Machine Tools Ltd** has requested access to gateway **FlashingLights_Wireless** (00:0D:8D:A6:00:B1) for **1** hour(s).

You have granted access to this user!

Notification of approval message displayed for vLOTO approver

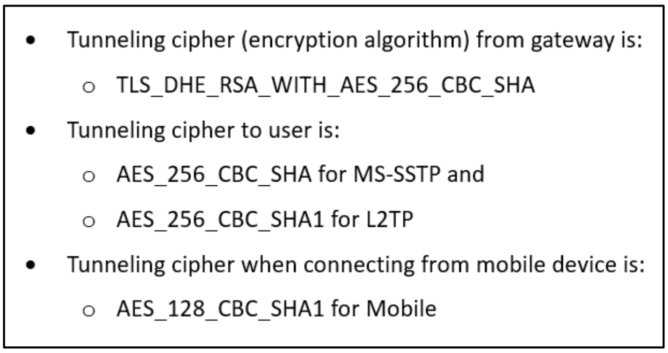
FlashingLights_Wireless
ProSoft ICX35-HWC
00:0D:8D:A6:00:B1

Remote user may now securely connect to gateway

Virtual Lockout-Tagout, when enabled – remote user must obtain permission to connect!

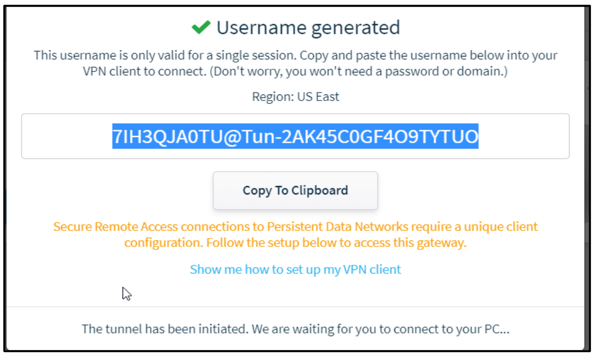
For example, if a system integrator has to connect to the packaging machine to troubleshoot, the SI must first request permission. The plant supervisor will receive the request to connect from the SI as an email. Once approved, the SI can connect and troubleshoot. The plant supervisor can remove all access at any time if needed. All vLOTO activity is logged, and is available to be exported and saved for future forensic use.

The last part of the device access security layer is connecting to the machine network. When the user connects to the machine network, an AES 256-bit encrypted tunnel is created between the user and the remote gateway via Belden Horizon. The gateway supports IP addresses on the machine network that the remote user can connect to.



- Tunneling cipher (encryption algorithm) from gateway is:
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- Tunneling cipher to user is:
  - AES_256_CBC_SHA for MS-SSTP and
  - AES_256_CBC_SHA1 for L2TP
- Tunneling cipher when connecting from mobile device is:
  - AES_128_CBC_SHA1 for Mobile

Data is fully encrypted!



✓ Username generated

This username is only valid for a single session. Copy and paste the username below into your VPN client to connect. (Don't worry, you won't need a password or domain.)

Region: US East

7IH3QJA0TU@Tun-2AK45C0GF4O9TYTUO

Secure Remote Access connections to Persistent Data Networks require a unique client configuration. Follow the setup below to access this gateway.

The tunnel has been initiated. We are waiting for you to connect to your PC...

Tunnel passwords are random and automatically generated!

Belden Horizon uses SSTP (Secure Socket Tunneling Protocol) to create the tunnel. SSTP uses port 443, so there is only one port to open and manage.

Dynamic Tunnel passwords are automatically generated 32-byte one-time passwords per user connection and per gateway. One-time use passwords are another key security feature, as the same password cannot be reused. This minimizes the threat of “man-in-the-middle” attacks since stealing the session password will not enable an attacker to open another tunnel with that password later on. The activity log records all tunneling events.

The next layer of security addresses security of data. As stated earlier, the connection between the remote user and the gateway is fully encrypted. Belden Horizon does not monitor, interpret, or store any user application data like a PLC program or a HMI file. Data is encrypted end-to-end, including the communication between the microservices in AWS. Belden Horizon account data at rest in the cloud is also encrypted. The cloud security controls are reviewed monthly.

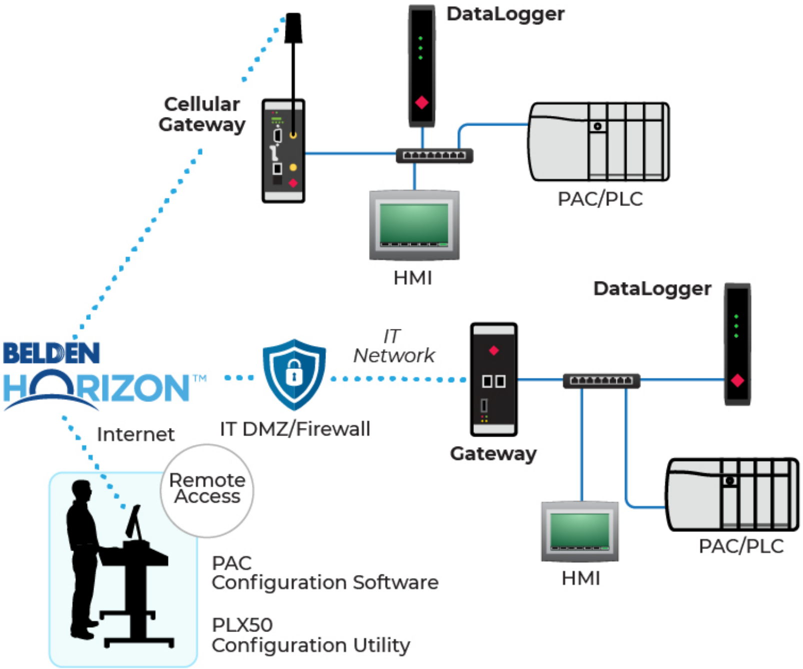
The final layer of security is the **platform**, Belden Horizon. The platform leverages the power of AWS to enhance security and reliability. There are multiple regional tunnel servers located strategically around the globe to minimize latency when a remote user connects to a gateway. The tunnel servers are fully redundant: Belden Horizon supports a dedicated data plane for communications between gateways (used for PDN applications), and a control plane for device management and remote user connection. The platform undergoes regular internal and third party security evaluations to ensure it is always secure.

Connecting to a Machine, Quickly, and Securely, using Belden Horizon

Secure remote access (SRA) or secure machine access (SMA) is a remote user connecting to a specific machine or a section of the plant to troubleshoot a problem or for maintenance.

To connect to the remote machine:

- User logs into Belden Horizon by going to https://www.belden.io. If Single Sign-On (SSO) or 2FA has been enabled on the account, then the user will need to log in appropriately
- User then opens the Project and selects the Gateway to connect to. If vLOTO has been enabled, the user requests approval to connect to the gateway. Once approval has been granted, the user initiates connection to the Gateway.
- Follow the prompts to connect to the gateway. Once connected, the remote user will be able to communicate to the end device like the HMI or PLC using the device's configuration software.
- On completion of the task, disconnect to close the SRA session.



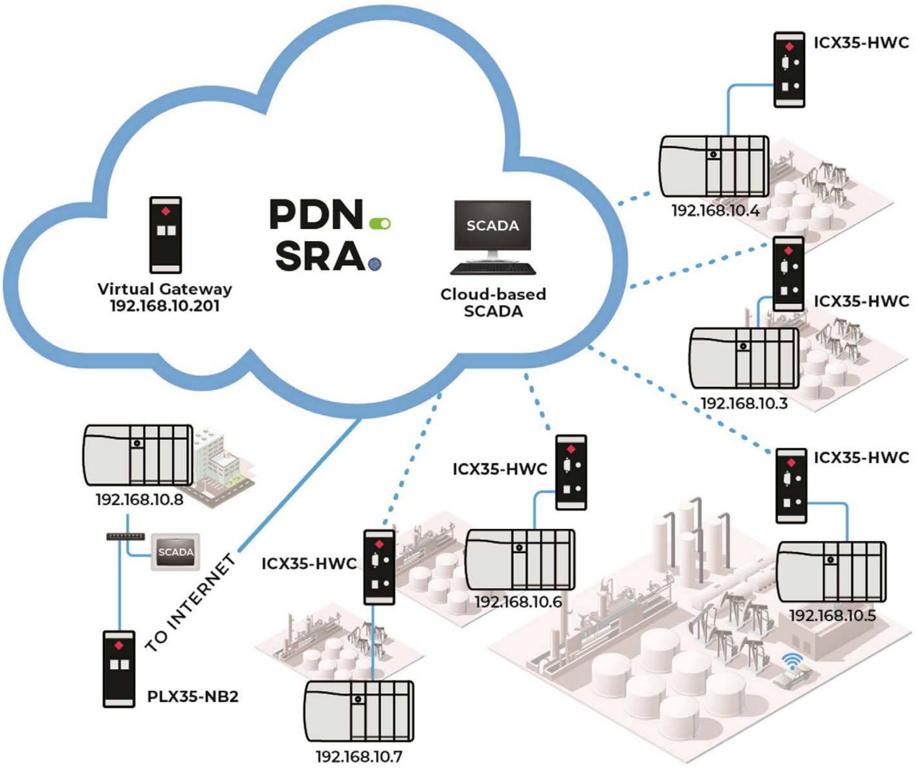
Reduce downtime and support costs with Belden Horizon's Secure Remote Access to the machine.

Always-on Connectivity to Remote Assets

PDN, or Persistent Data Network, is an always-on connection. PDN works by establishing a permanent and secure VPN connection between geographically dispersed locations for a SCADA-type network. Belden Horizon does all of the heavy lifting and the maintenance of the PDN network is invisible to the user. The security policies and rules required to manage a secure PDN network are fully automated. PDN is always available (>99%) and continuously secure. A PDN network requires a minimum of two gateways, and the VPN data is pooled.

To create the PDN network:

- Activate the cellular and/or wired gateways in the correct Belden Horizon account
- User logs into Belden Horizon by going to https://www.belden.io. If Single Sign-On (SSO) or 2FA has been enabled on the account, then the user will need to login appropriately
- User creates a PDN Project and adds the Gateways to this Project. Once the Gateways are added to the Project, the PDN network is automatically created and managed.

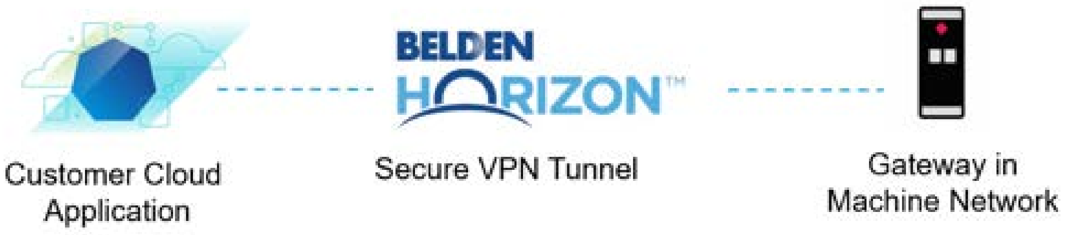


Some of the benefits of the PDN network include:

- Co-existence of cellular and wired gateways in a single network. So, if the main control center has internet access, then the user can use the wired gateway.
- Remote sites with cellular gateways are carrier-agnostic. That is, one site can use Verizon, while another site can use AT&T. This is not possible with carrier-based M2M networks.
- Peer-to-peer communications between the sites. That is, the sites can communicate to a central location or in-between them, reducing the reliance on a master location.

Persistent Data Network (PDN) to Cloud Connectivity

The always-on, permanent, and secure VPN connection between geographically dispersed locations isn't just valuable for traditional SCADA-type networks, but also for networks with cloud-based SCADA or IIoT (Industrial Internet of Things) intelligence. In these applications, the Virtual Node container can be installed in the customer's cloud application instance, which provides the gateway connection to the PDN network.



Summary

Belden Horizon is simple, secure, and managed. It is designed for OT professionals to help improve productivity and profitability when troubleshooting machines or a process, or to connect remote assets to a central SCADA system. The platform can be used by IT to backup OT data (example: configuration or log files) to an IT network for backup without have to create a link between the OT and IT network Belden Horizon is easy to use and secure. It deploys defense-in-depth with five layers of security, including AES 256-bit encryption, Single-Sign-On, token-based 2FA, and the use of secure socket tunneling protocol (port 443) for remote connection to the gateway. Belden Horizon is cloud-native, fully redundant, and always available.

To learn more about Belden Horizon, contact your local **ProSoft Distributor** or **ProSoft Representative.**