# DATASHEET

## Belden Horizon™ Console

**ProSoft Technology®**

The Belden Horizon™ Console is part of Belden's suite of software for industrial solutions. It is an IT-secure and OT-friendly solution that allows users to establish safe, reliable, and secure communications anywhere in the world.

Using Belden Horizon's unique EasyBridge™ technology, automation programming tools (such as Studio 5000®, Unity® Pro, TIA Portal, and many more) can talk directly to automation devices without the need to set up IP routing or other complicated communications settings. Belden Horizon's EasyBridge™ technology makes it simple and secure for remote sites to communicate with each other. Its Edge Orchestration feature allows users to deploy and manage edge applications across multiple edge devices at the same time from anywhere.

The Belden Horizon Console uses a zero-trust multilayered approach to security. These include single sign-on, Virtual Lockout-Tagout, two-factor authentication, IP allow list, role-based user and device access, user-configurable password policies, and encrypted tunnels.

The Belden Horizon Console is:
- Designed to manage multiple users, gateways, and users intuitively and easily
- Mobile-ready with a dedicated app available for download on the iOS platform.
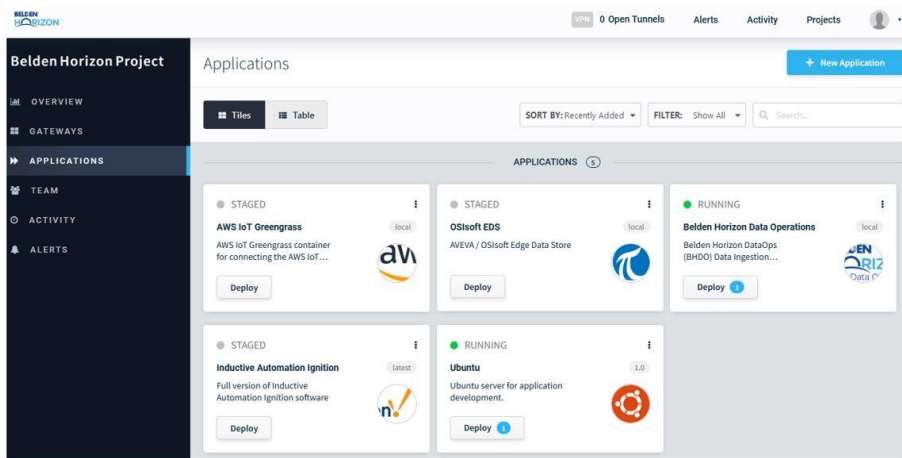- Available as SaaS service hosted by Belden and on-premises

The on-premises option allows the deployment of the Belden Horizon Console within the user's environment for either a private cloud, public cloud, or datacenter with an installed virtualization platform. Supported virtualization platforms include, but are not limited to VMware ESXi and Nutanix AHV.
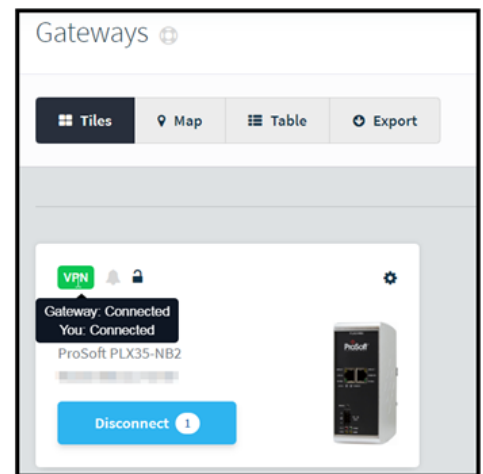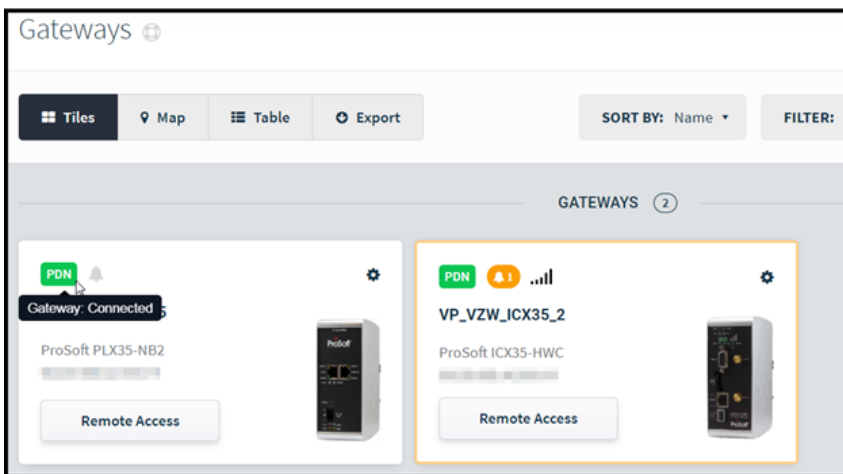
# Edge Orchestration

The Belden Horizon Console's Edge Orchestration feature allows users to deploy and manage edge applications across multiple edge devices at the same time from anywhere. The application can be provided by Belden or the user.

This feature allows applications to be seamlessly and securely deployed to edge devices such as Belden's OpEdge-4D and OpEdge-8D edge gateway devices.



| Main Features | Customer Benefits |
|---|---|
| • Supports the management of edge applications across one or more devices<br>• Enables the onboarding, monitoring, and updating of containers on edge hardware | • Empowers users to easily implement, install, and integrate with various industrial applications, regardless of the vendor |

The Belden Horizon Console allows the creation of two types of remote connections:



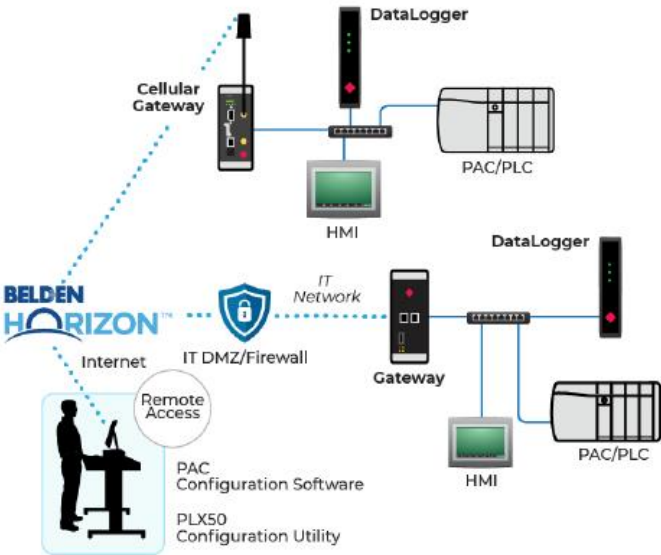| Always-On Connection<br>called Persistent Data Network (PDN) | On-Demand Connection<br>called Secure Remote Access (SRA) |
| --- | --- |
|  |  |
| This type of remote connection is used to connect geographically dispersed locations for a SCADA type network, like monitoring a municipal water utility or a gas distribution network. PDN is like being plugged into a local switch. | This type of remote connection is for a specific purpose. Examples include checking status, changing PAC software, or upgrading firmware. The user will disconnect once the action has been completed. |
| **Main Features**<br>• Managed network with tunnel connections between the connected gateways and tunnel server<br>• Configurable Layer 2 or Layer 3 connectivity<br>• Compatible with Prosoft Technology Gateways & Virtual Node | **Main Features**<br>• Virtual Lockout-Tagout (vLOTO™)<br>• Two-factor authentication<br>• IP Allowlist<br>• Ability to extend one-time-use credentials |
| **Benefits**<br>• Grants a simple and secure remote communication network to connect geographically dispersed assets<br>• Establishes a communication network that is "always-on"<br>• Integrates to customer's cloud via Virtual Gateway | **Benefits**<br>• Allows access to remote equipment easily through creation of secure tunnels<br>• Provides significant security (e.g. IP Allowlist) and safety (e.g. vLOTO™) benefits for remote OT assets<br>• Reduces downtime and support costs |
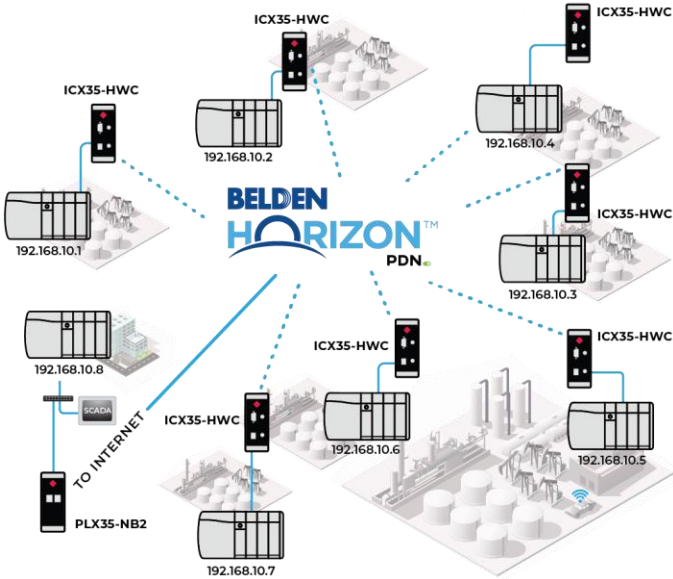
# Security

All communications with the Belden Horizon service use HTTPS for site authentication and data encryption. Gateways are activated in the Belden Horizon Console using a two-step authentication. All gateway connections are initiated by the gateway to prevent a spoofed service from initiating a gateway connection. No user-installed software is required, which eliminates potential "watering hole" attacks and time-consuming software patch maintenance.

## Advanced Two-Factor Authentication (2FA)

With advanced two-factor authentication, users can be confident that only registered users can access the account. When advanced 2FA is enabled, users must enter a username, password, and a unique time-based one-time password. The time-based, one-time password is auto generated via an authenticator app on the user's phone.

## User-Configurable Password Policy

With a configurable password policy, users can determine password complexity requirements and mandatory rotation periods in line with existing policies. Configurable policy rules include enforcing minimum password length, password expiration period, requiring alpha-numeric characters and more.

## Single Sign-On (SSO)

Single sign-on allows users to access multiple applications with one set of credentials. With SSO, IT can manage user access to improve security and productivity. SSO uses SAML 2.0. SSO works by sending the login request to a known federated identity provider (IDP) and the credentials are checked against the organization's active directory server. If the credentials are correct, then the user will be allowed to access the application.

## Virtual Lockout-Tagout (vLOTO™)

With Virtual Lockout-Tagout, authorized plant personnel control when and how their machines are remotely accessed. The Belden Horizon Console user requests access for a specific period, which the authorizer(s) must approve. The authorizer does not need to be a Belden Horizon Console user – they can be an IT manager, plant engineer, shift supervisor, or other authorized person. The authorizer(s) can deny or revoke access at any time. Companies can also access a thorough activity log of permissions, acceptances, and denials to meet security requirements.

## IP Allow List

Access specific IP addresses when remotely connected to the gateway.

## Managed Network – Bridged or Routed

PDN is intended to enable quick and easy SCADA style applications. A PDN is a collection of ProSoft Technology gateway endpoints that participate in one Layer 2 network or in separate networks which establish a Layer 3 routing between the regional tunnel server and the gateways. The Belden Horizon Console manages the tunnel connections between the gateway and the tunnel server.

Using the Belden Horizon Console's unique EasyBridge™ technology, automation programming tools (such as Studio 5000®, Unity® Pro, TIA Portal, and many more) can communicate directly to the automation devices.

## VPN Tunneling

The cloud to gateway connections in the PDN network are IPSec over HTTPS. In a PDN network, the Belden Horizon Console provides an AES256 encrypted VPN connection between the sites.

EasyBridge Secure Remote Access provides an AES256 encrypted VPN connection between the user's PC and the network connected to the Belden Horizon Console. VPN uses SSTP (the standard tunneling method) or L2TP client with IPSec encryption to minimize security vulnerabilities of third-party VPN client software.

## User Accounts and Access Control

The Belden Horizon Console Organization owner and project administrators can invite team members to join projects in the organization.

Access control for users is managed by the account administrator. Users are assigned rights to administer, connect, and configure gateways, or to connect only. An Organization Owner can transfer ownership of remote access devices (for example, a machine builder granting ownership to an end user once the OEM no longer needs control of the equipment).

## Project Based User Interface

Gateways and users are organized into Projects within the Belden Horizon Console organization. All gateways added to a PDN Project are either connected to form one Layer 2 network (single subnet) or divided into independent subnets using Layer 3 Routing. Automation devices connect to this network through the gateways and communicate with each other. Each organization requires a PDN subscription.

## Data Ingestion & Analytics in Cloud

In combination with a Virtual Node appliance (a soft gateway) available in the Belden Horizon Console, transferring data into Cloud environments is made easy.

This virtual appliance can be deployed to a cloud-based or on-premises server to enable data ingestion and analytical applications.

## Ethernet/Cellular Connections

Outbound connections from gateways use HTTPS only. Client VPN connections use SSTP via TCP port 443 or L2TP via ports 500, 4500, and 1701.

## Subscriptions

Ideal for system integrators and machine builders who rely on the Belden Horizon Console to service their customers. Subscriptions are modular so they can be ordered to fit as needed and be very cost effective. Whether remote access to a remote site is required or a Persistent Data Network, features can be enabled on an "as needed" basis.

# Technical Overview

The CAIQ (Consensus Assessment Initiative Questionnaire) v3.1 framework governs our security policies, 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 the Belden Horizon Console's connectivity architecture with the cipher suites information.

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

# Subscription Information

| Feature/Service | Description | BHC Cloud-based Service https://belden.io | BHC On-Premise Infrastructure |
|---|---|---|---|
| SRA (Secure Remote Access) Per 1 Gateway | • On-demand, secure access to remote assets on OT networks through ICX35-HWC, PLX35-NB2.<br>• 2 gateways are included free of charge | BHC-CLD-SRA | BHC-ONP-SRA |
| PDN (Persistent Data Network) Per 1 Site/Gateway | • Create a secure, Always-On connection (Layer 2 or layer 3) between two sites using ICX35-HWC, PLX35-NB2, or a virtual gateway<br>• Includes SRA Functionality | BHC-CLD-PDN | BHC-ONP-PDN |
| Edge Orchestration | • Remotely deploy and manage edge applications on edge compute devices like OpEdge-8D and OpEdge-4D.<br>• Include SRA and PDN functionality | BHC-CLD-EDGE | BHC-ONP-EDGE |
| Basic Features | • Number of projects: 25<br>• Number of users: 25<br>• Concurrent connections: 6<br>• Tunnels per project: 6<br>• SRA Projects: 2 | (Included) | (Included) |
| Advanced Features | • vLOTO™ Customer-defined password policy<br>• Single User, Multiple Orgs Single Sign-On<br>• Allow list<br>• Role-based user / device access<br>• Access based on protocol, port number, and MAC ID | (Included with paid subscription of SRA, PDN or Edge Orchestration) | (Included with paid subscription of SRA, PDN or Edge Orchestration) |
| Cloud Data Storage | Cloud data storage cumulatively utilized by features like Edge Orchestration | BHC-CLD-STR | (N/A) |
| Cloud Data Transfer | • Cloud data transfer cumulatively utilized by features like SRA, PDN, Edge Orchestration.<br>• Data pool per Organization | BHC-CLD-XFR | (N/A) |
| **On-Premise only** | | | |
| Installation Services | • Initial installation services for deploying BHC On-Prem in customer's environment<br>• Includes one year of maintenance | (N/A) | BHC-ONP-BASE |
| Maintenance | Annual maintenance (including minor enhancements and bug fixes) | (Included) | BHC-ONP-MAINT |