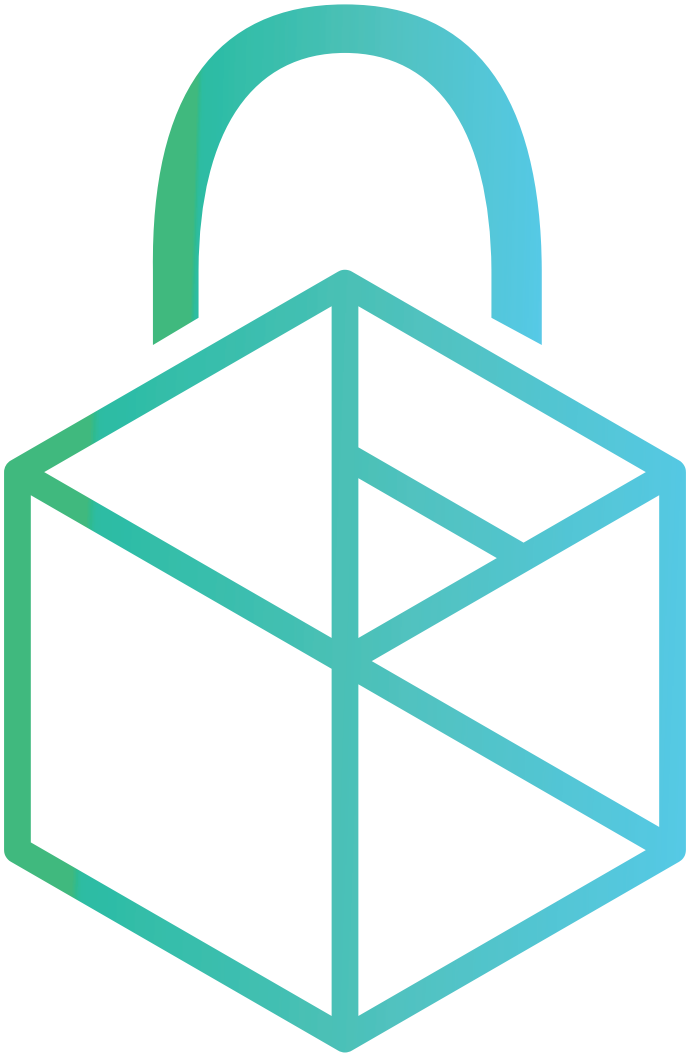
BifrostConnect Security Documentation

Version 2.0



bifrostconnect.com

Table of Contents

Under the hood

BifrostConnect is a hardware-based remote access solution ("BifrostConnect Solution") that allows secure remote access without installing software on the endpoints. The solution enables access to IT and OT equipment and devices, including but not limited to computers, PLCs, mobile phones, IoT devices, and network equipment.

The solution offers the following session types:

KVM Access: Keyboard, Video, and Mouse control of the endpoint, ensuring that data is processed and kept on-premises.

IP Tunnel: Zero Trust IP communication between remote devices without VPN Tunneling.

Serial Tunnel: Direct Serial (RS232) connection between remote devices.

USB Tunnel: Direct USB connection between remote devices.

SSH: Access the endpoint through the Secure Shell Protocol in a terminal.

Serial Terminal: Console access via a serial connection to the on-premises Terminal.

Offline File Transfer: Transfer files to offline devices without exposing endpoints to the internet.

The BifrostConnect Solution consists of the following components:

1. The **Bifrost Unit** is a compact remote-control unit.

2. The **Services** provide session authentication, session bridge, web-based session interface, identity and access management, audit logging, and API integrations.

The BifrostConnect Solution enables secure (i) remote access to, (ii) remote control of, and/or (iii) remote connection between IT equipment and devices (each a "Remote Device"). Remote access sessions are controlled via a browser-based web client, ensuring that no remote access software is required. The web client can also activate a relay remotely, typically used for remote reboot operations. These modes of operation can be viewed as all the same from a security perspective because the information exchanged in all modes happens in the same peer-to-peer (P2P) encrypted context based on Web Real-Time Communication (WebRTC).

Technology Overview

- BifrostConnect Service is currently hosted on Digital Ocean using Docker containers.

- Web-based Authentication by Auth0
  (You can read more about Auth0 security here) https://auth0.com/security

- End-to-End encrypted data session (Mouse, Keyboard, and Video streaming) over WebRTC over TURN servers (this/these can be customer hosted)

- End-to-End encrypted messages over MQTT using secure WebSocket's (wss)

- Custom authentication layer on top of MQTT

- HTTPS (TLS) on all web clients and web-facing endpoints

Zero Trust by Design

BifrostConnect is a secure way to access private endpoints and applications without needing a VPN or Remote Access Software. Our innovative approach is based on an adaptive trust model that grants access on a "need-to-know" basis, defined by granular policies. Combining hardware and cyber security, BifrostConnect adds an extra layer of protection to safeguard your high-value assets.

BifrostConnect's 5 Z approach

1. Zero Trust Management

BifrostConnect allows your company to choose a dedicated Admin who is empowered to establish security and Access Management policies. Emphasizing the principles of just-in-time access and granular policies, BifrostConnect delivers precision access control to specific endpoints and applications on a one-to-one basis, effectively minimizing risk and enhancing security.

For seamless integration, access management can be aligned with the organization's existing Identity and Access Management (IAM) solution. Furthermore, BifrostConnect supports audit logging for usage tracking and event monitoring. This log data can be conveniently integrated with the organization's Security Information and Event Management (SIEM) systems for streamlined security management.

2. Zero Unit Configuration

Your BifrostConnect Solution is dedicated and pre-configured to your organization, enabling them to be directly shipped and installed at the desired location or endpoint. These Units provide secure remote access right out of the box, eliminating the need for on-site specialist intervention for configuration.

To maximize security, Bifrost Units retain access and security policies even in the event of hardware resets. Your organization's unique Bifrost Manager handles all security policies, and Bifrost Units are safeguarded from local web interface access and configuration, ensuring your BifrostConnect Solution remains uncompromised.

3. Zero Software Installs

The deployment of the BifrostConnect Solution requires no software installation on endpoints, facilitating a seamless integration process. The user can control where endpoint data is processed, depending on the type of session connection. This flexibility allows for on-premises data processing or data communication between endpoints if permitted. This feature empowers remote operators to utilize 3rd-party software on their own computers to interact with the remote endpoint during tunnel sessions. This facilitates a smooth and efficient remote operation experience.

4. Zero Internet Exposure

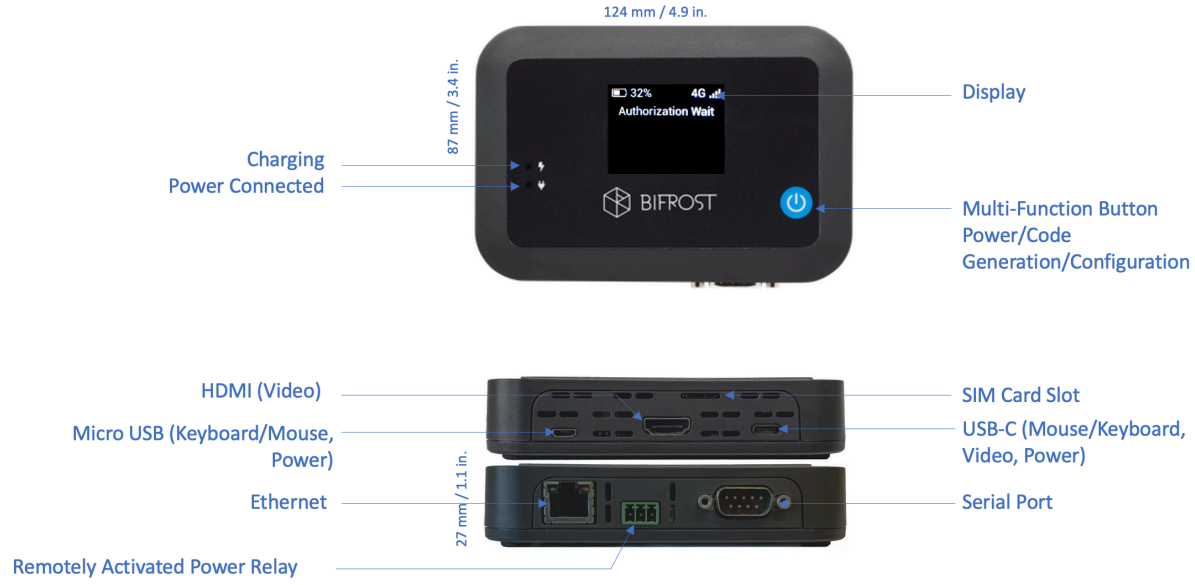
Bifrost Units utilize internet connections either in-band or via the integrated out-of-band connection. Crucially, these units do not share the internet connection with the endpoints during a Remote Access Session, ensuring secure and undisturbed communication channels.

5. Zero Network Compromise

Advancing on the principles of Zero Trust Network Access (ZTNA), BifrostConnect decouples application access from network access. This reduces your attack surfaces, inhibits lateral movement, and ensures that access to endpoints and applications is exclusively granted to authorized users, hence eliminating implicit trust.

Leveraging inside-out connections from the Bifrost Unit to the user, the solution effectively renders endpoints and network infrastructure invisible to unauthorized users. IP addresses remain hidden from unauthorized users and the internet, ensuring your network remains secure and inaccessible.

Hardware Security



The Bifrost Unit

The Bifrost Unit operates on an Industrial embedded Linux and is fortified with regular security patch updates through Over-the-air (OTA) technology. The Linux core is stripped of all non-essential services, and only those required for the BifrostConnect Service are installed. Therefore the only listening port on the Bifrost is 443.

Several security measures have been implemented to ensure the physical and digital security of the Bifrost Unit.

1. To prevent alteration of the Bifrost Unit after firmware loading, the only way to modify the signed firmware is through an OTA update. Changing settings occurs via encrypted MQTT/WebRTC through the BifrostConnect Services.

2. There are no physical service ports or debugging interfaces on the Bifrost Unit, and no local users exist on the internal Linux platform. Furthermore, uniquely generated device keys are generated with the least privilege and can be revoked.

3. All fuses on the PCB are burnt, preventing booting from alternative storage or devices.

4. Direct IP or Serial communication to reach the Bifrost Unit, such as SSH, is impossible, as no services are installed, and no local web services exist on the Bifrost Unit.

Firmware Upgrades

Firmware upgrades are only possible via the BifrostConnect Service. Each Bifrost Units firmware version is monitored by the BifrostConnect Service and is displayed in the BifrostConnect Manager.

If the firmware version of a Bifrost Unit is not current, the BifrostConnect web interface will display a prompt to update it, thereby ensuring optimal performance. The user can click the button, which sends a message to the Bifrost Unit, letting it know there is a new firmware update to download.

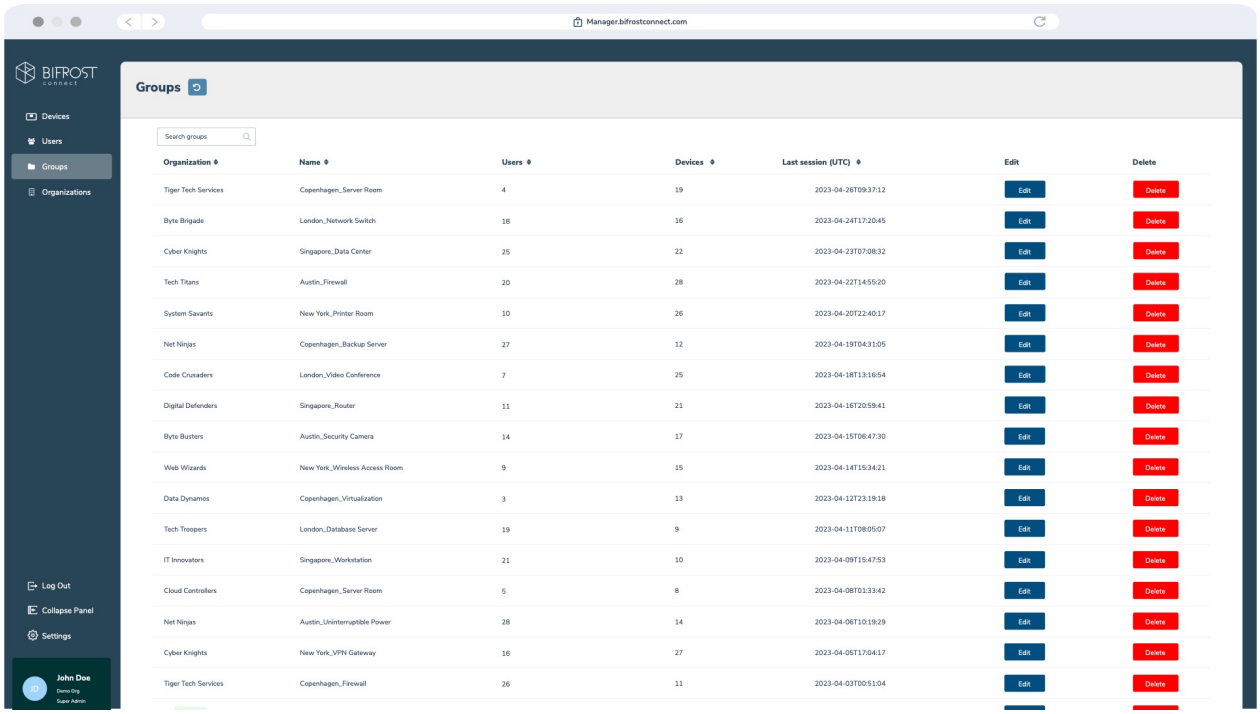
When initiated, the Bifrost Unit registers the update request. To ensure that the ongoing session is fully functional, the firmware update is postponed until session termination. When the session is terminated, the Bifrost Unit downloads the new firmware over HTTPS, verifies the signed firmware, applies it, and restarts.

Unit Variations

Each Bifrost Unit is explicitly produced as either an Attended or Unattended Unit. This selection is embedded in the unit, thereby ensuring the chosen role remains consistent throughout the lifespan of the product.

As a result of this variation, Attended Units are inaccessible in Unattended Sessions, and similarly, Unattended Units cannot be accessed during Attended Sessions. A deeper explanation of the distinction between Attended and Unattended Access is detailed in the Session Authentication section.

Bifrost Manager



Identity and Access Management

Least Privilege

The principle of least privilege ensures that every user or system is granted the minimum access levels necessary to fulfill their tasks or responsibilities. This approach restricts access to sensitive data and resources, reducing the risk of data breaches and cyber-attacks. If a user or program is compromised, the attacker's activities are limited to the privileges of that compromised user or program.

Just-in-Time

The "Just-in-Time" principle ensures that access is granted as needed and only for a duration necessary to complete a specific task or function. This ensures that access permissions are only active during the timeframe of need, minimizing the window of opportunity for attackers to exploit these privileges. Once the task is completed, the session is terminated. If the Operator wishes to reconnect, a new session with valid authentication is required, further reducing the possibility of unauthorized access or lateral movement within the network.

User Roles & Groups

Within the BifrostConnect Manager, a feature enables the definition of user policies. This functionality can be utilized to establish guidelines and regulations for user behavior and access privileges.

ACTION	*PRIVILEGED USER*	*ADMIN*
Initiate Sessions	In Group	In Organization
Operate Sessions	In Group	In Organization
Create Groups	–	✓
Add Users to Groups	–	✓
Add Devices to Groups	–	✓
View Users	–	✓
Create/Delete Users	–	✓

Manager Authentication

Standard MFA

The BifrostConnect solution incorporates Auth0's multifactor authentication, an industry-leading security service committed to the highest standards of protection. Auth0 employs a multitude of advanced strategies and technologies, such as continuous security monitoring, automatic threat mitigation, and regular third-party audits, ensuring the reliability and integrity of the multifactor authentication process. This robust security infrastructure supports our commitment to providing a secure, reliable, and user-friendly solution.

Learn more about Auth0: https://auth0.com/security

Single Sign-On (SSO)

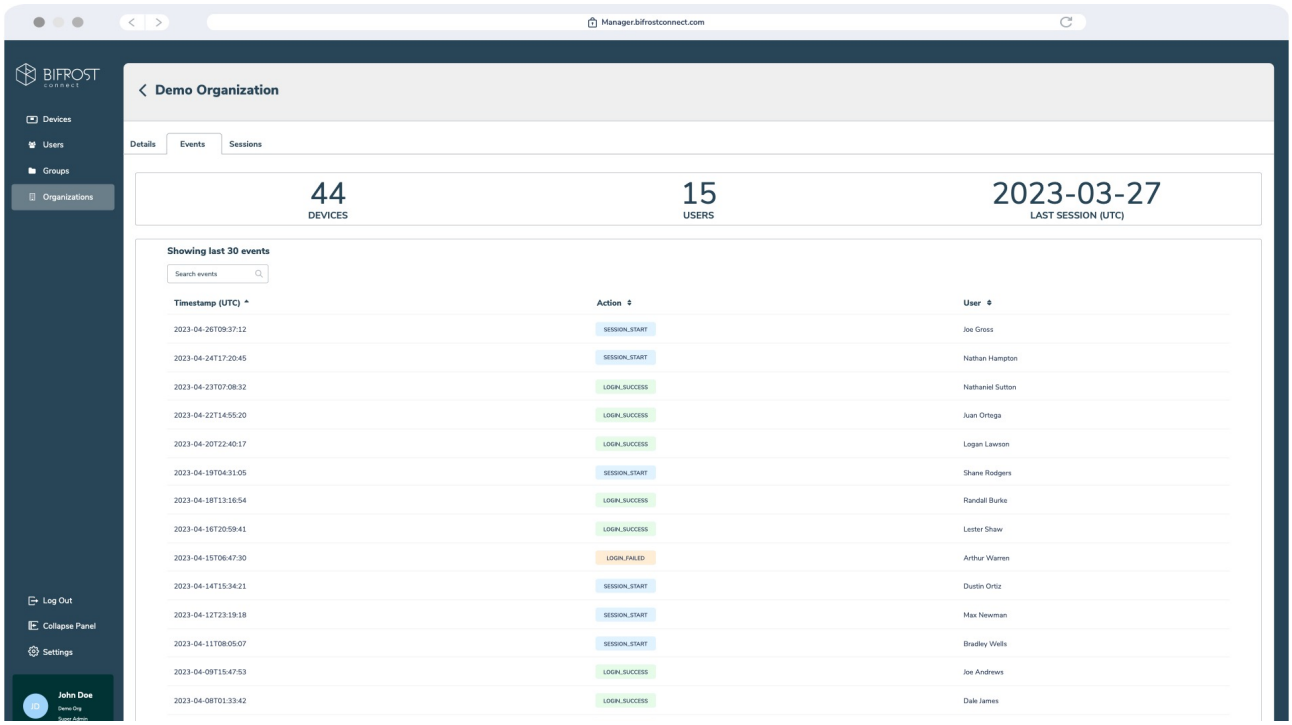
BifrostConnect supports Single Sign-On (SSO) for clients utilizing private BifrostConnect infrastructure, enhancing user convenience without compromising security. This integration allows users to securely access the entirety of your applications and services suite through a single login, eliminating the need to remember separate credentials for each service. When authentication is required, users are seamlessly redirected to the designated authentication domain. Should the user already be logged in, they are immediately redirected back to the original domain without needing re-authentication.

Protocols supported:

- SAML
- OAuth2
- AD/LDAP

Learn more about SSO: https://auth0.com/docs/authenticate/single-sign-on

Audit Logging



BifrostConnect offers comprehensive Audit Logging capabilities within the Manager to facilitate continuous monitoring and detailed documentation of activities across the client organization. This feature empowers users with the ability to track, record, and review actions, enhancing transparency and promoting accountability within client infrastructure.

Telemetry data

BifrostConnect Service receives the following telemetry data from the Bifrost Unit:

- Session duration
- Session count
- IP address assigned to Bifrost by DHCP/WAN
- Timing of user logins on gotobifrost.com (without specifying the connected Bifrost Unit)
- Most recent online status of Bifrost Unit
- List of nearby WIFI access points (SSID)
- Battery status and 4G signal strength
- Data traffic statistics for 4G and BifrostConnect Service usage
- Unique serial number/name of the Bifrost Unit
- Location based on cell tower (not GPS)

Privacy

All data in transit between the Bifrost Unit and the BifrostConnect Service/web session is encrypted, ensuring no user data is retained on either the Bifrost Unit or the service. Additionally, WIFI passwords are preserved in a hashed format on the specific Bifrost Unit but are not stored within the BifrostConnect Service.

Our privacy policy is available at https://bifrostconnect.com/privacy-policy/

SIEM Integration

BifrostConnect supports Security Information and Event Management (SIEM) Integration for clients utilizing the private BifrostConnect infrastructure. This technology compiles event log data from numerous sources, promptly detects unusual activity through real-time analysis, and initiates corrective measures. SIEM provides organizations with vital insights into their network activity, enabling a rapid response to potential cyber threats and compliance adherence.

Remote Access Sessions

Session Management

To ensure security and prevent impersonation of clients and Bifrost Units, the BifrostConnect solution employs robust access control measures. Each web client and Bifrost Unit is provided with a unique namespace for identification. A record of paired web clients and Bifrost Units is created by the BifrostConnect session manager, which precludes a Bifrost Unit from establishing connections with multiple web clients. Regular status messages are exchanged between web clients and Bifrost Units. Sessions are cleanly terminated through disconnect messages or, in the absence of status messages over a certain period, the service will terminate the session.

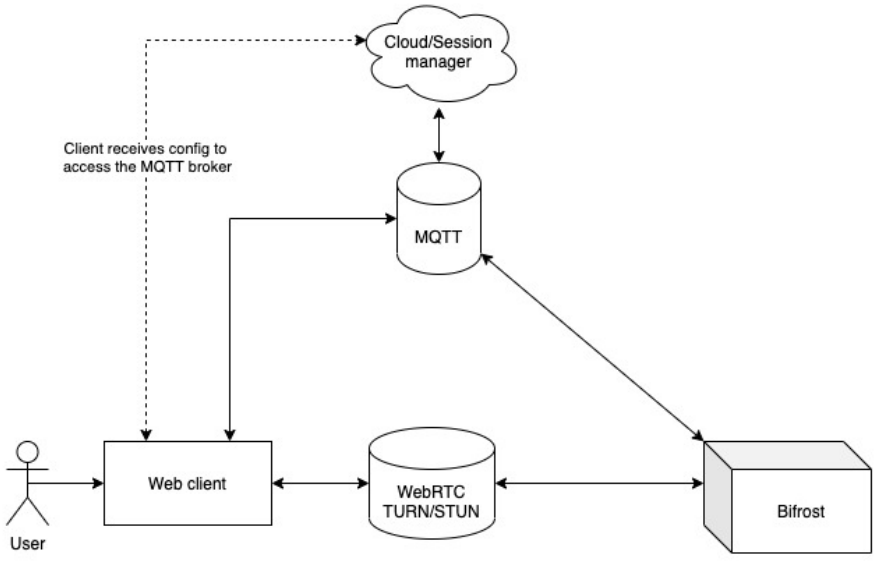
WebRTC interaction occurs exclusively between the web client and the Bifrost Unit, with the BifrostConnect Service facilitating the necessary WebRTC signaling only when a session is active. Post-session termination, the web client and Bifrost Unit independently terminate the WebRTC connection, independent of the BifrostConnect Service.

WebRTC Facilitation

WebRTC necessitates facilitation through a TURN server, typically called an ICE server. This process enables WebRTC to work with firewalls and, if needed, the transition from UDP to TCP packets.

The WebRTC standard requires the use of an out-of-band signaling system for trust establishment, peer identification, and other operational specifics, such as selecting a video codec. Our cloud session system delivers this requisite signaling.

The ICE server, utilizing the embedded TURN server, forwards the packets. Importantly, these packets are encrypted end-to-end to ensure the utmost data security.



In the BifrostConnect solution, both the web client and the Bifrost Unit authenticate themselves to the BifrostConnect Service, communicating over industry-standard encrypted channels utilizing Transport Layer Security (TLS). This encryption is separate from the peer-to-peer (P2P) encryption that occurs between the web client and the Bifrost Unit, which is secured via Datagram Transport Layer Security (DTLS) encryption through WebRTC.

WebRTC is a robust technology commonly used in online conferencing systems such as Microsoft Teams, Google Meet, among others.

While the BifrostConnect Service facilitates these P2P sessions and maintains the ability to terminate such sessions, it's important to note that it does not have the ability to access user-driven content within a P2P session. This is due to the DTLS encryption being negotiated directly between the web client and the Bifrost Unit, ensuring an additional layer of security.

Protocols and Firewalls

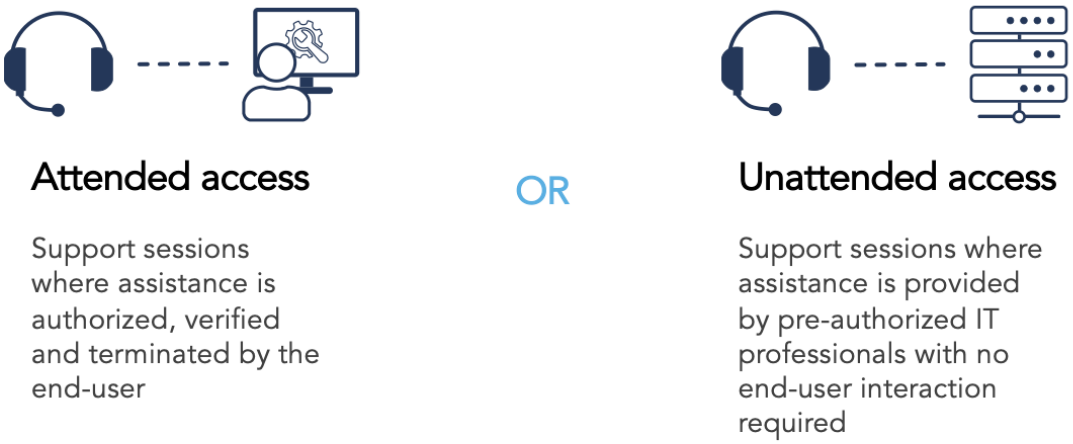
The solution employs a mix of TLS-encrypted secure WebSocket and HTTPS traffic for communication with the BifrostConnect Service and DTLS-encrypted peer-to-peer traffic between the web client and a Bifrost Unit.

The BifrostConnect Service's traffic encompasses HTML and javascript pages for the user interface, a select number of REST API endpoints for managing access tokens, and an MQTT-based publish/subscribe messaging channel over TLS WebSockets. Primarily, the security of the BifrostConnect Service's access control is bolstered by the MQTT access control layer, ensuring communication only occurs on authorized message topics.

Regarding external firewalls positioned between the web client and the BifrostConnect Service and between the Bifrost Unit and the BifrostConnect Service, the only apparent communication is HTTPS traffic via port 443 to various subdomains of gotobifrost.com, and WebRTC traffic, which includes access to TURN servers. This ensures UDP-based WebRTC traffic can pair endpoints and pass through the Firewall. As most web conference systems leverage the same technology, it's likely that corporate firewalls are already configured to accept this type of traffic.

Session Auth

The BifrostConnect Solutions comes in two versions:



Despite the solution's fundamental consistency, the protocols and guidelines regarding security, trust, and authentication are tailored to meet the specific needs of each use case.

Attended Access

Attended Access requires an on-site person to initiate remote access between the connected device and the Operator seeking to access the device remotely.

Attended Access utilizes Time-based One-time Password (TOTP) technology generated by a physical press on the BifrostConnect Unit. The generated password is displayed on the Unit screen and changes every 30 sec. To establish a session, the Operator must log in to gotobifrost.com (also MFA protected) or the Manager, enter his/her credentials, and then enter the eight-digit password (TOTP). The on-site person can disconnect the session anytime by pressing a button on the Unit.

Unattended Access

Unattended Access can be initiated by the operator without the need for an on-site individual.

Access to Unattended Access is gained through the Manager. By default, the Manager authentication process involves a combination of user credentials and multi-factor authentication (MFA), such as a Time-based One-time Password (TOTP) delivered through a trusted authenticator app.

Session Types

Each of the session types adheres strictly to the advanced security measures provided by WebRTC and BifrostConnect Zero Trust principles tailored for our sessions. These principles underline our commitment to ensure the following:

Zero Trust by Default: The Solution follows the principles of least privilege and Just-in-Time Access to ensure maximum security. Furthermore, all session data is encrypted by default and transitory.

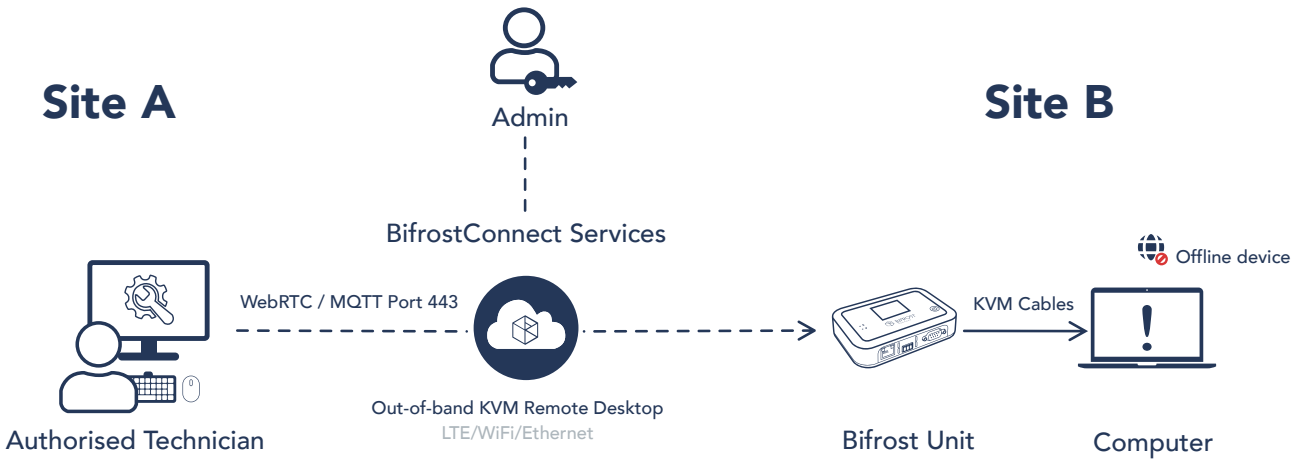
Zero Network Compromise: For added security, sessions can be established Out-of-band via cellular, if preferred.

Zero Software Installs: The Solution is Plug-and-Play, requiring no software installations. This accelerates implementation and usage while leaving the integrity of your endpoints untouched.

Zero Internet Exposure: Bifrost Units do not share the internet with endpoints during remote access sessions, ensuring added security.

This approach forms the foundation of our session types, emphasizing our commitment to a secure, streamlined, and seamless user experience.

KVM Access



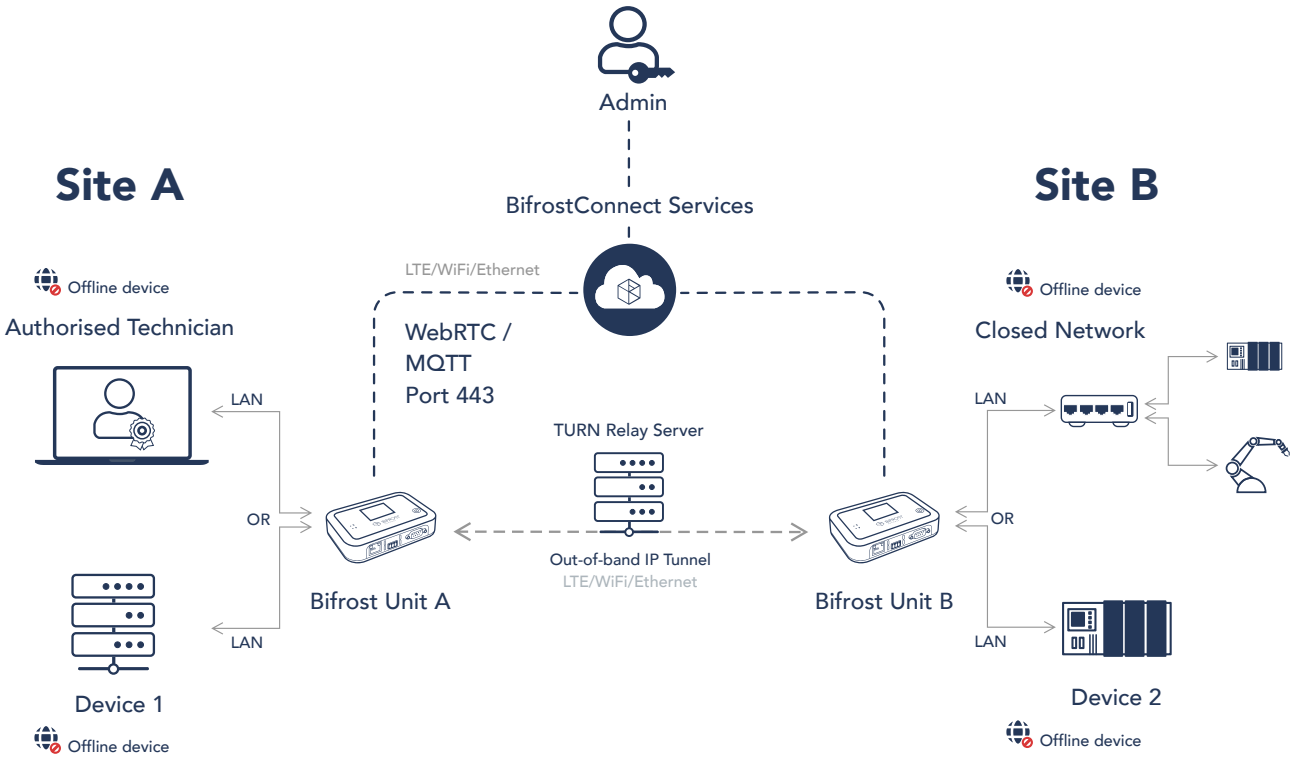
KVM Access Sessions facilitates the transmission of keyboard, video, and mouse (KVM) I/O signals. KVM Access leverages standard I/O communication protocols, thus eliminating the need for driver installations when interfacing with a Bifrost Unit. In situations where the Bifrost Unit uses in-band internet connections via LAN, the network connected to the unit cannot be modified or controlled, as the unit solely uses the network for establishing a connection to BifrostConnect Services and necessitates DHCP or a static IP.

Initiating a KVM Access Session requires the privileged user to authenticate via a multifactor-protected web interface, as detailed in the Session Authentication section. Any operation performed during a KVM Access Session is processed locally, ensuring data never leaves the security perimeter.

BifrostConnect does not endow the operator with additional user rights beyond those conferred by the organization's internal IT administration or security policies. For example, if a remote device is password-protected during login or boot-up, the operator must authenticate using their credentials.

The USB Key Storage Emulation feature, available during KVM Access Sessions, permits operators to mount the Bifrost Unit's 6GB internal storage as a USB Key for transferring files from the storage to the endpoint. However, KVM Access Sessions do not support remote file transfers or facilitate clipboard copy-paste functionality. The Bifrost Unit's internal storage is compatible with local encryption tools like BitLocker.

IP Tunnel



The Bifrost IP Tunnel is designed to provide a secure end-to-end encrypted connection between two Bifrost Units. These Point-to-Point tunnels are created on a per-session, on-demand basis, and all session data is transitory and will not be stored on any server.

Advancing upon Least Privilege principles, IP Tunnel Sessions can only be initiated by Users or Admins with requisite permissions. These privileged users are tasked with specifying the IP addresses and ports to be enabled for remote access during the session.

In the technical illustration, the Bifrost Unit at Site A is set up as the IP/Port forwarding destination. At Site B, the Bifrost Unit is set up as the IP/Port forwarding Source. As the master or receiving end, Site A initiates either Pull or Push requests during sessions. This selection can be adjusted dynamically.

Upon initiation and configuration, endpoints connected to the Bifrost Units at Site A and Site B form a closed network, allowing communication only with the IPs and Ports defined by the privileged user. Other Users with access to the device at Site A can operate the equipment without needing user credentials, which could be exploited after Session Termination.

Endpoint IP addresses are never exposed to devices, applications, the internet, or unauthorized users through the IP Tunnel, as all traffic is communicated via the IP address of the Bifrost Unit at Site B. Furthermore, it is not possible to perform a network scan of the endpoints through a Bifrost IP Tunnel.

For optimal security, equipment at both sites can be kept offline, enabling Air-gapped Remote Access. If a user desires simultaneous access to another private endpoint or from a different device, privileged users can spin up separate IP Tunnels.

In scenarios where devices are offline or behind a firewall, inside-out connectivity shields the network from the internet while still allowing application access to individual endpoints within the network.