WHERE VPNS END, BIFROST **CONNECT**

SECURING **REMOTE ACCESS** FOR CRITICAL INFRASTRUCTURE IN 2026 AND BEYOND

OVERVIEW

The purpose of **BifrostConnect**

Standing VPN tunnels and traditional network-based access methods are not suited for commissioning, incident response & 3rd party access in critical infrastructure.

Instead, we offer BifrostConnect Unified Out-of-Band Access that provides Secure transport, Native Endpoint Control & Session Governance in one unified platform that's:

1. Danish hardware-based remote access for both IT and OT
2. Made for commissioning, operational resilience and incident response.
3. The solution enables remote access that maps to NIS2 and IEC 62443 by minimizing persistent exposure and enforcing zero-trust controls.

USE CASE OVERVIEW

WHEN AND WHERE TO USE

	PROBLEM	SOLUTION	BENEFITS
COMMISSIONING	Often needed before the site network, IAM and IT exist; VPNs need standing network access and a client, and remote-desktop tools install software on the engineering station.	Clientless DNA (serial/KVM/SSH) over the Unit's own 4G; nothing installed on the asset, no network to join.	Bring gear online even before the site network or identity is in place, approved on site, with zero footprint on the asset.
PLANNED & AD-HOC MAINTENANCE	VPNs and persistent tunnels leave a standing, always-open path with broad subnet access that is hard to scope or time-bound, and unmanageable across many vendors.	Zero Standing Privilege: on-demand, subnet-scoped sessions, time-bound on Dedicated Cloud; approvals and access events logged in Manager and forwarded to SIEM.	Least-privilege access (a core NIS2 and IEC 62443 expectation) with no open door between sessions.
INCIDENT RESPONSE + EMERGENCY ACCESS	When the incident *is* the network or IT/IAM itself (ransomware, routing down, captive portal, IdP outage), VPNs, jump hosts and SSO-dependent tools fail exactly when needed.	Network-independent OOB path (own 4G/LTE) and self-contained identity in Manager (no dependency on your IAM); DNA reaches device consoles even when production routing is down.	A way back in that survives the incident, because it shares no fate with production or IT.

MADE IN DENMARK

BIFROST connect

THE COMPLETE SOLUTION

Technology Overview

MANAGER = Central Control Plane
- Session scheduling, JIT access control/ Time-based Access, audit logging.
- Forced 2-factor authentication
- Secure Filetransfers (Direct and Offline)
- Cloud or On-prem

NB. Signalling only / no production data stored or accessible through cloud or TURN-servers:
BifrostConnect has no ability to decrypt customer production data. Sessions use end-to-end encrypted WebRTC (DTLS-SRTP); our TURN relays forward only ciphertext, and no production data is persisted in our cloud.

Remote Technicians

Hardware-Enforced Access (Attended / Unattended Bifrost Unit)

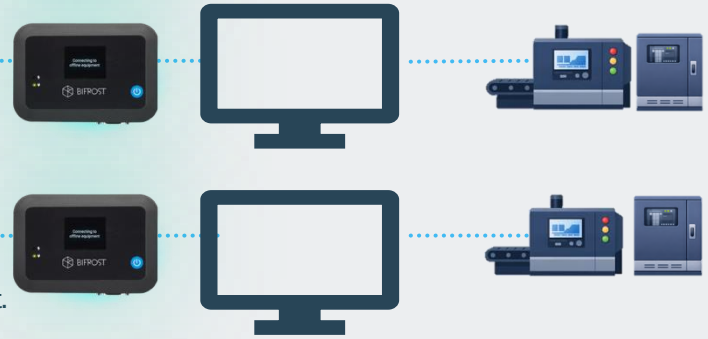
On-site GPC device, Engineering Station or OT system / machine.

CLIENTLESS 1-2-1 ACCESS

DIRECT NATIVE ACCESS (DNA) aka "The Worlds Longest Virtual Arms":
Browser-based hardware-level console access via WebRTC.
Single Bifrost Unit connected to target equipment. No software installation on either side.

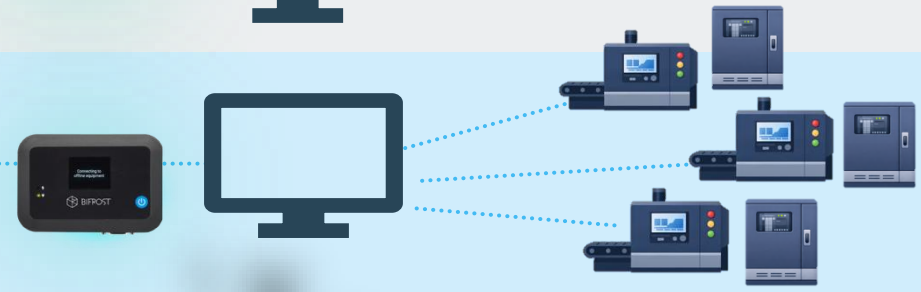
CLIENTLESS TUNNEL ACCESS (CTA) aka "The Closest Thing You get to Air-Gapped Tunnelling": a pure hardware-to-hardware encrypted tunnel - no software on either side, only active while the session is live

DIRECT CLIENTLESS TUNNEL ACCESS (DCTA) aka "The most ad-hoc HW-based tunnel available": Browser-based tunnel client. Single Bifrost Unit in the OT environment.
No software installation required - runs entirely in the operator's browser.



LIGHT-WEIGHT APP FOR 1-2-1, MULTI-ENDPOINT AND MULTI-TECHNICIAN ACCESS

DIRECT TUNNEL ACCESS (DTA) aka "The Worlds Longest Cable":
WireGuard-based IP tunnel via lightweight installed client application, connecting to a Bifrost Unit in the OT environment. Subnet mappings enable access to multiple endpoints.



2026 SESSION ACCOUNTABILITY

SessionGuard:
- Session governance with mandatory live-streaming + recording of technician PC screen and keystrokes during sessions.
- Streamed and saved on customer owned and controlled logserver.

AccessGuard (AG):
Station-level access governance with local MFA, scoped application access, and endpoint-side session recording

MOSED USED ACCESS TYPES

DNA vs DTA

Direct Native Access + Attended Unit

Direct Native Access (DNA):
Aka "The World's Longest Arms":
Browser-based hardware-level console access via WebRTC. Single Bifrost Unit connected to target equipment. No software installation on either side.

MANAGER - Central Control
(Private environment on common cloud, private Dedicated Cloud or On-prem)

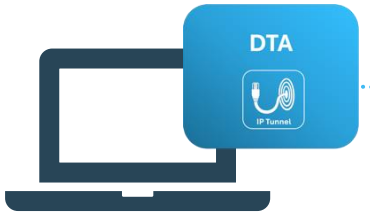
NB. Signalling only / no production data stored or accessible through cloud or TURN-servers:
BifrostConnect has no ability to decrypt customer production data. Sessions use end-to-end encrypted WebRTC (DTLS-SRTP); our TURN relays forward only ciphertext, and no production data is persisted in our cloud.

(Only outbound on port 443)

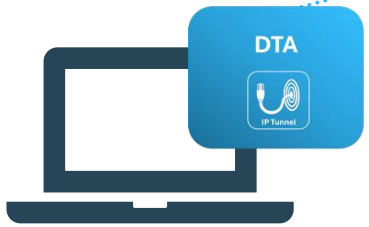
Attended Access Unit:
Hardware-Enforced Access with built-in TOTP function for on-site physical control.

HDMI/USB — Server / PC
SSH — Linux Server
RS232 — Router

Direct Tunnel Access + Unattended Unit

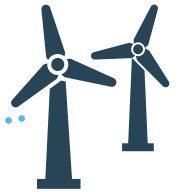


DIRECT TUNNEL ACCESS (DTA) aka "The World's Longest Cable":
WireGuard-based IP tunnel via lightweight installed client application, connecting to a Bifrost Unit in the OT environment. Subnet mappings enable access to multiple endpoints.



Unattended Access Unit:
Hardware-Enforced Access with forced 2-factor authentication and time-limited sessions controlled in Manager interface.

IP



On-site Engineering Station or OT system / machine e.g. PLC

7 REASONS WHY CUSTOMERS CHOOSE US

1. **SECURE TRANSPORT, ENDPOINT CONTROL AND ENFORCED SESSION ACCOUNTABILITY IN ONE UNIFIED PLATFORM, PROVIDING YOU BOTH DEVICE-LEVEL AND NETWORK-LEVEL ACCESS TOGETHER.**
2. **OUT-OF-BAND HARDWARE ACCESS TO ANY EQUIPMENT:** Including air-gapped, legacy and OS-less assets no other remote access solution can reach.
3. **BUILT ON THE BELIEF THAT "OT CALLS OUT. OT NEVER RECEIVES": N**o open ports, no inbound traffic, no internet exposure of target equipment.
4. **Local on-site control + centralized governance: T**he facility owner controls who gets in, when, and for how long, without giving up central oversight
5. **ZERO TRUST BY DESIGN: M**andatory MFA, just-in-time sessions, least privilege, full audit trail and session recording - with no dependency on the vendor's engineering license.
6. **WORKS WHEN NOTHING ELSE DOES:** 4G out-of-band connectivity means remote access survives network outages, and the portable unit with built-in battery requires no infrastructure changes on site.
7. **"TRUE AD-HOC ACCESS BY NATURE":** "Ad-hoc" is not just a software add-on or something that's configured in order to work - it's the nature of the Bifrost Unit, to be moved around and plugged in where and when you need it.

MADE IN DENMARK