
# WHERE VPNS END, BIFROST **CONNECT**

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

BIFROST connect

THE PROBLEM

# Traditional network-based remote access is great, **until it isn't.**

### It works when everything is ideal

- Operations run smoothly and systems are fully patched
- An in-house IT team manages all access control
- No urgent need for third-party experts
- You can afford the downtime, or the breach

**But access breaks down when the standard solution can't do the job, or there is too much friction to get access:**

- Networks are isolated / equipment is offline
- Firewalls are closed, no OS or permanent connections
- Vendors need immediate ad-hoc access, but you shouldn't compromise cybersecurity, control or governance.
- An incident takes the standard solution offline

***So, people invent rogue workarounds that quietly raise risk.***

=

.. And for the days when this is not your reality, **you need BifrostConnect**

Danish, hardware-based remote access for ad-hoc third-party access in critical infrastructure.

**Built for where traditional network-based tools fail.**

THE ANSWER

# **BifrostConnect:** Unified Out-of-Band Access

### Reaches what others can't

Device and network-level access to air-gapped, legacy and OS-less assets that software- or network-based tools can't reach.

### Survives any outage

Connects over Ethernet, WiFi, 4G/LTE or Starlink, with no infrastructure changes on site.

### Outbound-only, Zero Trust

OT calls out and never receives: no open ports, no inbound traffic, plus per-session MFA, just-in-time, least privilege.

### Enforced accountability

Session recording with a full audit trail, independent of who owns the engineering license.



MADE IN DENMARK

BIFROST connect

WHERE IT FITS

# Where VPNs end, BifrostConnect =

1. **Air-gapped & offline**
   Closed networks where the internet and standard VPNs are blocked.

2. **Legacy & OS-less hardware**
   No network card, no OS, or Serial/USB-only troubleshooting.

3. **Strict security & compliance**
   When policy forbids third-party access to the internal network.

4. **Urgent third-party access**
   When AD, tickets and VPN setup are too slow for onsite needs.

5. **Safety-critical environments**
   When the site must keep on-site control of who connects.

6. **Vendor-owner conflict**
   A neutral, hardware-based bridge when no tool is agreed on.

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.

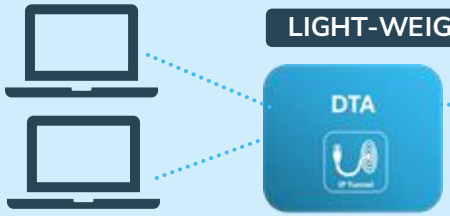
## CLIENTLESS 1-2-1 ACCESS


**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

HARDWARE AND SECURITY

# How Does The **Hardware** Work?


**Hardware Details:**

- 6 GB Internal storage
- Battery for around 1 hour session without charge
- Portable/Light weight, only 249 Grams
- Locked to Bifrost Cloud
- WIFI & LTE Modem built in.

# The Cybersecurity

**HARDWARE:**

- ✓ Hardened industrial embedded Linux, stripped to only the BifrostConnect Service.
- ✓ Firmware is signed and updated only over-the-air (OTA); all other settings change only via encrypted MQTT/WebRTC.
- ✓ No inbound services such as SSH or local web.
- ✓ No physical service or debug ports, no local users, and unique, revocable device keys.
- ✓ All fuses are burnt, so it cannot boot from alternative storage or devices.

**NETWORK:**

- ✓ Outbound only on port 443. No open ports, no internet exposure, inbound blocked.
- ✓ No connectivity sharing, no lingering sessions.

**ACCESS:**

- ✓ Mandatory per-session MFA and dedicated per-person login via the Manager portal.

**DATA:**

- ✓ End-to-end encrypted sessions (WebRTC, DTLS-SRTP).
- ✓ No production data stored or accessible via cloud or TURN; relays forward ciphertext only.

**ACCOUNTABILITY:**

- ✓ Immutable audit log (who, what, when).
- ✓ Enforced session recording and keystroke logging, regardless of license ownership.

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)

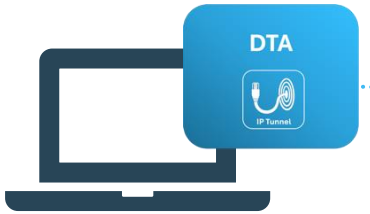

(Only outbound on port 443)

**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.

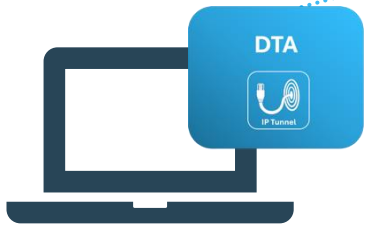

**Attended Access Unit:**
Hardware-Enforced Access with built-in TOTP function for on-site physical control.

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**

HOW IT WORKS

# Direct Native Access + SessionGuard

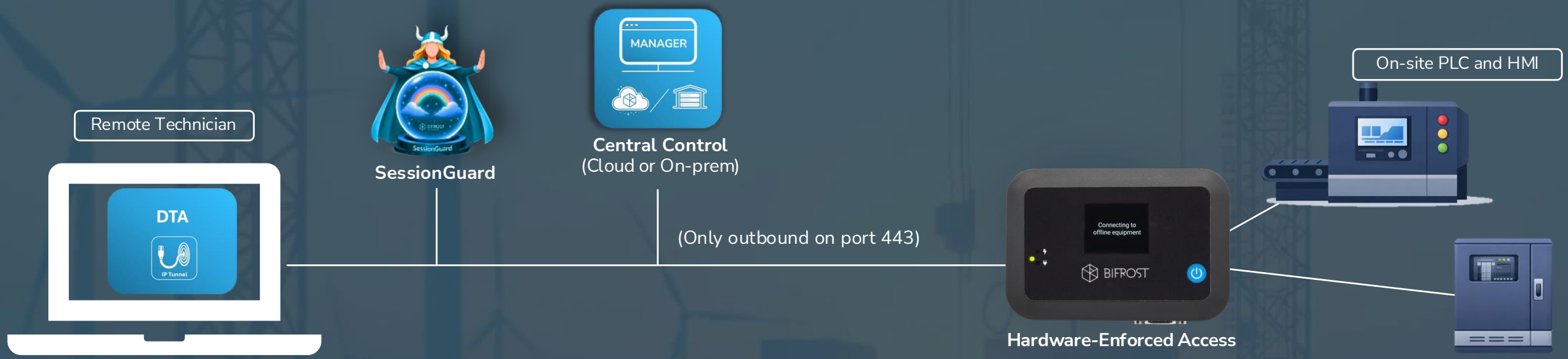
When Programming licenses are owned by the vendor / located on technician PC / VMware remote.


| ACCESS TYPE | SESSION GOVERNANCE | CENTRAL ACCESS CONTROL | HARDWARE-ENFORCED ACCESS |
|---|---|---|---|
| **Direct Native Access (DNA)**<br>Browser-based hardware-level console access via WebRTC.<br><br>Single Unit connected to target equipment/engineering station.<br><br>No software installation on either side.<br>(One 2 One communication) | **SessionGuard** (coming soon)<br><br>• Session governance with mandatory live-streaming + recording of technician PC screen and keystrokes during sessions.<br>• Streamed and saved on customer owned and controlled logserver.<br><br>**Best Practice:**<br>• **Vendor:** keep DTA+SG on Virtual Machine dedicated to the specific customer<br>• **Customer:** keep OT offline / in a closed network + don't use same vendor that controls the remote connection, to setup the log server. | **MANAGER:**<br>Central Control as private environment on common cloud, Own Dedicated Cloud, or On-Prem infrastructure.<br><br>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. | **Unattended Units:**<br>Enables seamless remote access through Bifrost Manager with multi-factor authentication (MFA) and a mobile app for identity verification. This allows authorized personnel to access equipment remotely, even when no on-site staff is available.<br><br>**Attended Units:**<br>Utilizes One-Time Password (OTP) technology, requiring a physical press on the Bifrost Unit to generate a secure authorization code. This ensures that only on-site personnel can authorize remote sessions, making it ideal for scenarios where access needs to be validated and terminated locally. |

HOW IT WORKS

# Direct Tunnel Access + SessionGuard

When Programming licenses are owned by the vendor / located on technician PC / VMware remote.




| ACCESS TYPE | SESSION GOVERNANCE | CENTRAL ACCESS CONTROL | HARDWARE-ENFORCED ACCESS |
|---|---|---|---|
| **Direct Tunnel Access (DTA):** WireGuard-based E2E encrypted IP tunnel via lightweight installed client application, connecting to a Bifrost Unit in the OT environment. Subnet mappings enable access to multiple endpoints.<br><br>- One 2 Many<br>- One 2 One<br>- Many 2 One | **SessionGuard** (coming soon):<br>• Session governance with mandatory live-streaming + recording of technician PC screen and keystrokes during sessions.<br>• Streamed and saved on customer owned and controlled logserver.<br><br>**Best Practice:**<br>• **Vendor:** keep DTA+SG on Virtual Machine dedicated to the specific customer<br>• **Customer:** keep OT offline / in a closed network + don't use same vendor that controls the remote connection, to setup the log server. | **MANAGER:**<br>Central Control as private environment on common cloud, Own Dedicated Cloud, or On-Prem infrastructure:<br><br>• Session scheduling, JIT access control, audit logging.<br>• Time-based access<br>• 2-factor authentication<br>• If based on Dedicated Cloud Infrastructure (on-prem is possible)<br>• Filetransfers (Direct and Offline)<br><br>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. | **Unattended Unit:**<br>Enables seamless remote access through Bifrost Manager with multi-factor authentication (MFA) and a mobile app for identity verification.<br><br>This allows authorized personnel to access equipment remotely, even when no on-site staff is available. |

HOW IT WORKS

# Direct Tunnel Access + AccessGuard

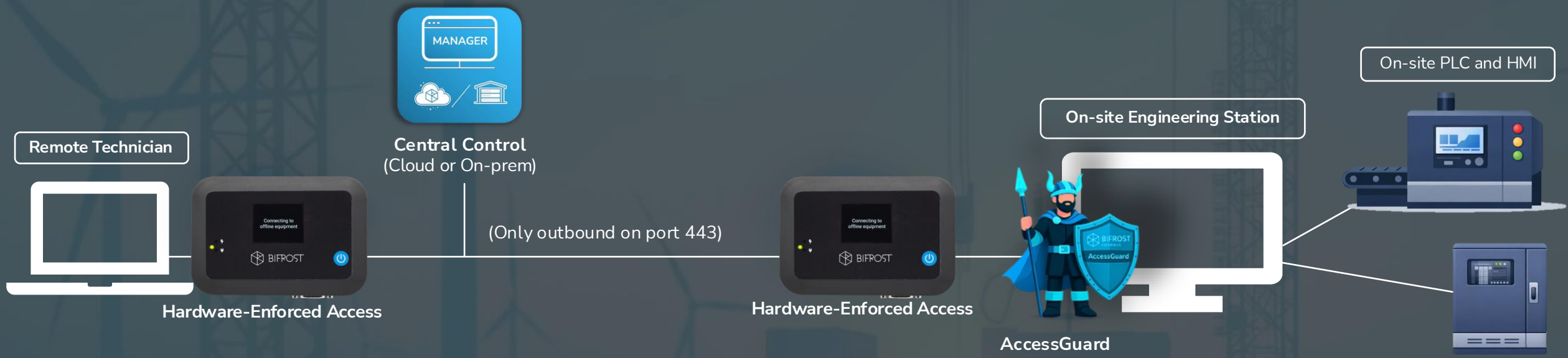
When Programming licenses are owned by the customer / located on engineering station on-site.


| ACCESS TYPE | SESSION GOVERNANCE | CENTRAL ACCESS CONTROL | HARDWARE-ENFORCED ACCESS |
|---|---|---|---|
| **Direct Tunnel Access (DTA):** WireGuard-based E2E encrypted IP tunnel via lightweight installed client application, connecting to a Bifrost Unit in the OT environment. Subnet mappings enable access to multiple endpoints.<br><br>- One 2 Many<br>- One 2 One<br>- Many 2 One | **AccessGuard** (coming soon):<br><br>Station-level access governance with local MFA, scoped application access, and endpoint-side session recording. | **MANAGER:**<br>Central Control as private environment on common cloud, Own Dedicated Cloud, or On-Prem infrastructure:<br><br>• Session scheduling, JIT access control, audit logging.<br>• Time-based access<br>• 2-factor authentication<br>• If based on Dedicated Cloud Infrastructure (on-prem is possible)<br>• Filetransfers (Direct and Offline)<br><br>**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.** | **Unattended Unit:**<br><br>Enables seamless remote access through Bifrost Manager with multi-factor authentication (MFA) and a mobile app for identity verification.<br><br>This allows authorized personnel to access equipment remotely, even when no on-site staff is available. |

HOW IT WORKS

# Clientless Tunnel Access + AccessGuard

When Programming licenses are owned by the customer / located on engineering station on-site

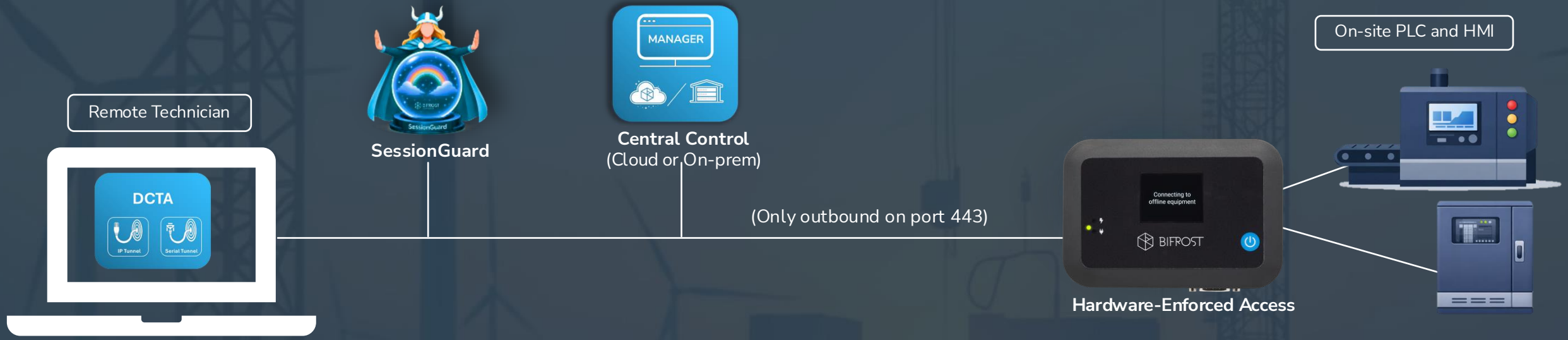



| ACCESS TYPE | SESSION GOVERNANCE | CENTRAL ACCESS CONTROL | HARDWARE-ENFORCED ACCESS |
|---|---|---|---|
| **Clientless Tunnel Access (CTA):**<br>A pure hardware-to-hardware encrypted tunnel - no software on either side, only active while the session is live.<br><br>- One 2 One communication | **AccessGuard**<br>(coming soon):<br><br>Station-level access governance with local MFA, scoped application access, and endpoint-side session recording. | **MANAGER:**<br>Central Control as private environment on common cloud, Own Dedicated Cloud, or On-Prem infrastructure:<br><br>• Session scheduling, JIT access control, audit logging.<br>• Time-based access<br>• 2-factor authentication<br>• If based on Dedicated Cloud Infrastructure (on-prem is possible)<br>• Filetransfers (Direct and Offline)<br><br>**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.** | **Unattended Units:**<br>Enables seamless remote access through Bifrost Manager with multi-factor authentication (MFA) and a mobile app for identity verification. This allows authorized personnel to access equipment remotely, even when no on-site staff is available.<br><br>**Attended Units:**<br>Utilizes One-Time Password (OTP) technology, requiring a physical press on the Bifrost Unit to generate a secure authorization code. This ensures that only on-site personnel can authorize remote sessions, making it ideal for scenarios where access needs to be validated and terminated locally. |

HOW IT WORKS

# Direct Clientless Tunnel Access + SessionGuard

When Programming licenses are owned by the vendor / located on technician PC / VMware remote, and they are not allowed to install software on their technician pc's.

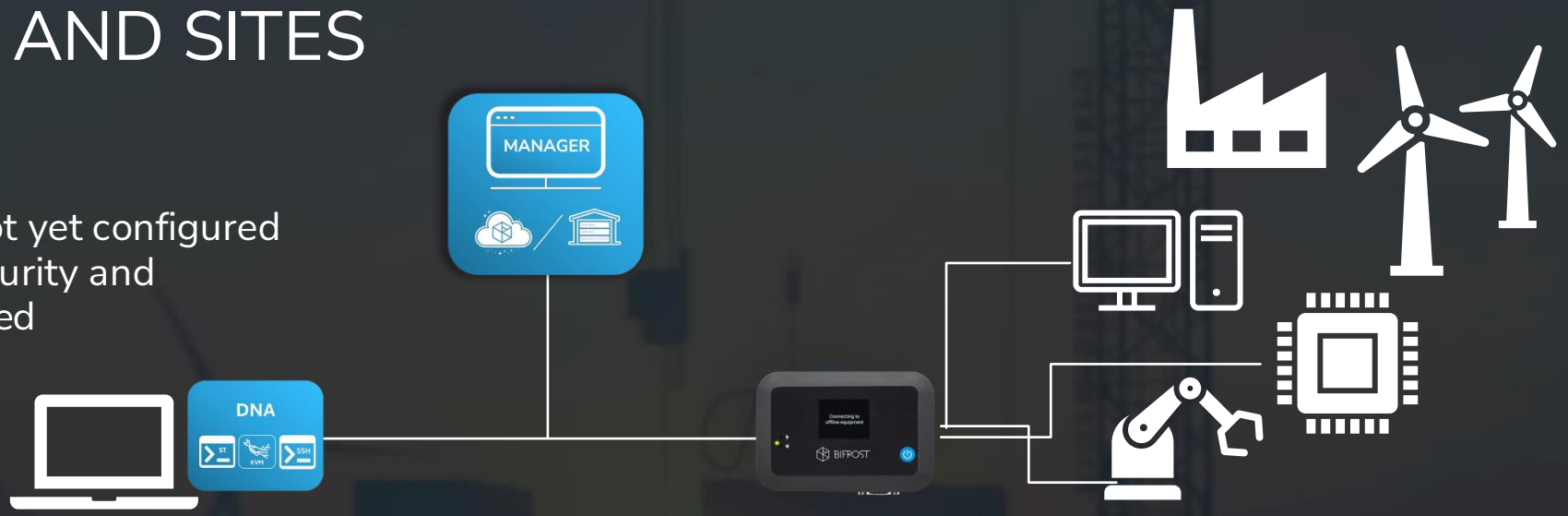



| ACCESS TYPE | SESSION GOVERNANCE | CENTRAL ACCESS CONTROL | HARDWARE-ENFORCED ACCESS |
|---|---|---|---|
| **Direct Clientless Tunnel Access (DCTA):**<br><br>Browser-based tunnel client. Single Bifrost Unit in the OT environment. No software installation required - runs entirely in the operator's browser. | **SessionGuard** (coming soon):<br>• Session governance with mandatory live-streaming + recording of technician PC screen and keystrokes during sessions.<br>• Streamed and saved on customer owned and controlled logserver.<br><br>**Best Practice:**<br>• **Vendor:** keep DCTA+SG on Virtual Machine dedicated to the specific customer<br>• **Customer:** keep OT offline / in a closed network + don't use same vendor that controls the remote connection, to setup the log server. | **MANAGER:**<br>Central Control as private environment on common cloud, Own Dedicated Cloud, or On-Prem infrastructure:<br><br>• Session scheduling, JIT access control, audit logging.<br>• Time-based access<br>• 2-factor authentication<br>• If based on Dedicated Cloud Infrastructure (on-prem is possible)<br>• Filetransfers (Direct and Offline)<br><br>**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.** | **Unattended Unit:**<br><br>Enables seamless remote access through Bifrost Manager with multi-factor authentication (MFA) and a mobile app for identity verification.<br><br>This allows authorized personnel to access equipment remotely, even when no on-site staff is available. |

USE CASES

# **COMMISSIONING** NEW SYSTEMS, PRODUCTION LINES AND SITES

- Networks are isolated or offline
- Operating Systems and IPs are not yet configured
- Vendors need fast access, but security and compliance cannot be compromised




**Challenge - Traditional Remote Access does not support:**

- **Initial device setup** (OS installation, IP configuration, etc.)
- **Device configuration and programming before network or internet connectivity is established**
- **Firmware upgrades that require reboots and pre-boot user interaction**

**What you need:**

**Native access** to offline equipment even during installation, reboot, etc.

**Out-of-band** 4G/LTE connectivity

**Portable Endpoint-Agnostic** solution that can provide direct access to any type of device.

**BifrostConnect Solution:**

By enabling secure remote access to offline and pre-commissioned equipment, we've helped organizations save hundreds of expert hours and cut the overhead of travel, visas, site training, and approvals. Projects move faster, safer, and with fewer dependencies.



MADE IN DENMARK

USE CASES

# ISOLATED **AD-HOC 3RD PARTY ACCESS,** WITH LOCAL CONTROL AND SESSION GOVERNANCE

**For when your primary remote access solution:**

- Is not connected / Fully Deployed
- Is too complex and time consuming
- Can't cover the requirements / isn't secure enough
- Takes too long to get "access"
- Has not been implemented

**Then we protect both OT x IT environment:**

- Old legacy systems
- No internal IT personnel
- Limited Resources
- Increasing Demands for Cybersecurity best practice
- For when the only alternative is sending an expert on-site


**With Ad-Hoc access, the security model shifts from "open by default" to "closed by default."**



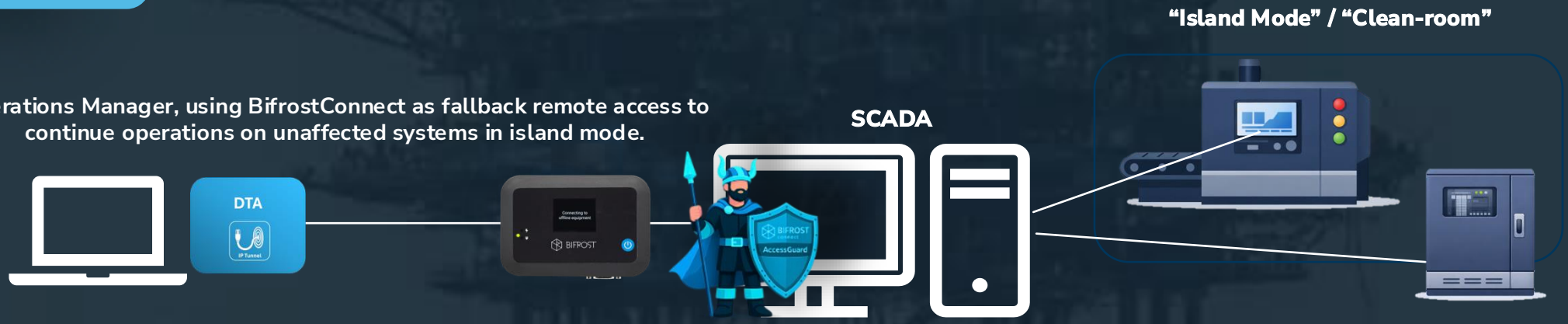
MADE IN DENMARK

USE CASES

# BUSINESS **CONTINUITY,** INCIDENT **RESPONSE** & DISASTER **RECOVERY**

## The Result

- ✓ Maintain business continuity
- ✓ Enable remote diagnostics during containment
- ✓ Recover systems safely and efficiently
- ✓ Restore operations without exposing OT to the internet




MADE IN DENMARK

USE CASES

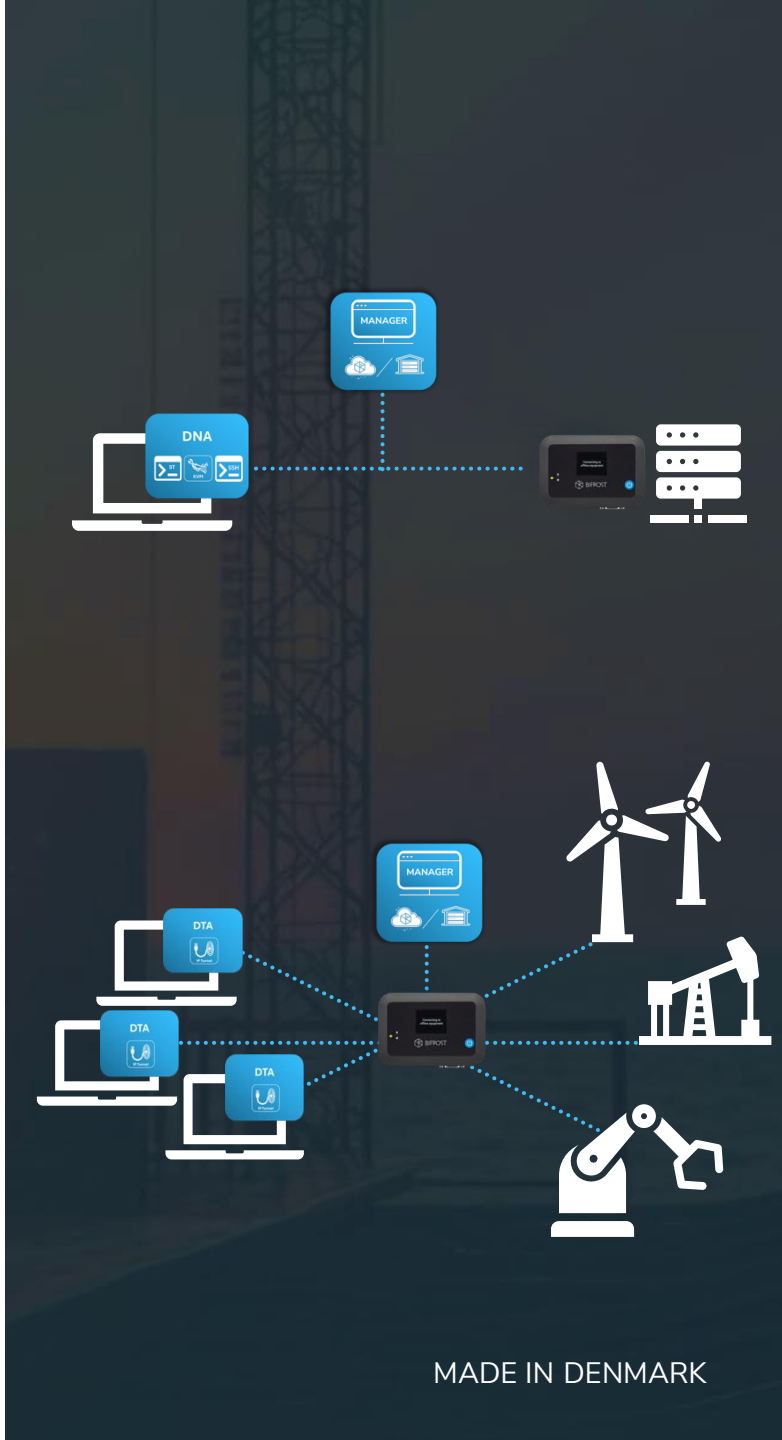
# ADDITIONAL EXAMPLES

## Ad-Hoc Remote Access for Server Recovery and Remote Configuration

| SITUATION | BifrostConnect implementation | WHY THIS FITS |
|---|---|---|
| ▪ Ad-hoc need for fast remote access to customer sites<br>▪ Server recovery and remote configuration tasks<br>▪ Single IT technician per session | ▪ Unattended Unit<br>▪ Direct Native Access (clientless KVM, Serial, SSH, no client on the technician PC)<br>▪ Bifrost Manager, Advanced plan | ▪ No software install on technician PC or target server<br>▪ Sessions initiated remotely via Manager with MFA, no on-site dependency<br>▪ Outbound-only OT posture, no inbound ports, no internet exposure<br>▪ Full audit log, individual identity per session |

## Remote Access for Multiple Users Across Remote Sites, *With session management and per-user audit*

| SITUATION | BifrostConnect implementation | WHY THIS FITS |
|---|---|---|
| ▪ Multiple users and user groups needing remote access to different customer sites and different equipment<br>▪ Portfolio of remote sites<br>▪ Session management and per-user audit required for compliance | ▪ Unattended Bifrost Units (one per site)<br>▪ Direct Tunnel Access (identity-bound, time-scoped IP access)<br>▪ Bifrost Manager, Advanced plan<br>▪ SessionGuard (Beta - pre-access included upon availability) | ▪ Multi-user governance with hierarchy-based access<br>▪ Time-bound just-in-time sessions<br>▪ Audit log per session for compliance evidence<br>▪ Time-limited OTP authentication<br>▪ Visibility into access and usage patterns |






MADE IN DENMARK

# 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