BEST PRACTICE GUIDE

BEST PRACTICE GUIDE - PART 2:

Implementing the best-practice framework for 3rd party access to OT, with BifrostConnect

JUNE 2026, PART 2 - VERSION 1.21

Companion to Part 1, with Product Mapping, Architecture and Implementation Hardening Guidance.

BIFROST connect

TABLE OF CONTENTS

ABOUT THIS PUBLICATION

Implementing the OT Best Practice Framework with BifrostConnect

Part 2 - Product mapping, architecture, and implementation hardening guidance

June 2026
Part 2, Version 1.21

Published by BifrostConnect

This document is the companion to the OT Best Practice Guide, Part 1 (June 2026). Part 1 describes the vendor-neutral best practice framework. Part 2 describes how a BifrostConnect deployment satisfies the requirements in Part 1.

FIGURE 1. BifrostConnect product family at a glance

One platform: 3 access methods, governance and recording, on a single hardware hub.

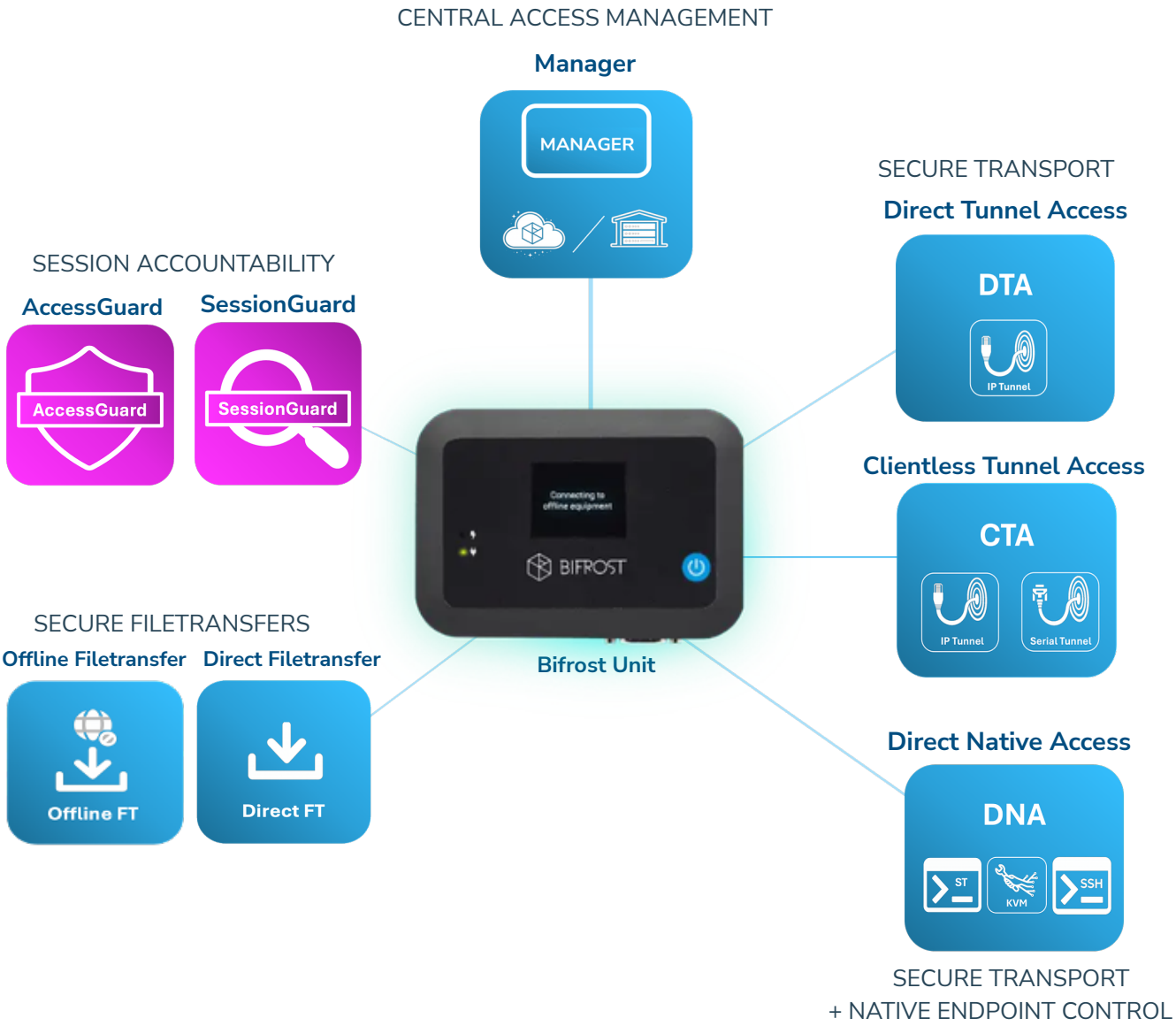


Figure 1. BifrostConnect product family at a glance. One platform, three access methods, governance and recording in a single hub.

Three access methods: Direct Native Access (KVM/Serial/SSH, clientless browser-based), Direct Tunnel Access (IP, installed lightweight client), and Clientless Tunnel Access (IP/Serial, hardware-to-hardware Bifrost-to-Bifrost air-gapped paths). Two additional file-transfer modes, Direct File Transfer and Offline File Transfer, cover vendor file movement. The full product reference table appears later in this document.

ABOUT THIS COMPANION DOCUMENT

This is Part 2 of a two-part publication by BifrostConnect. Part 1 is a vendor-neutral best-practice framework for third-party access to operational technology, written to stand alone as a reference for threat modelling, scenario analysis and regulatory mapping.

This Part 2 is the implementation companion: it describes how to deploy BifrostConnect, so the controls Part 1 calls for are delivered securely, what each deployment decision means for the resulting evidence chain, and where to harden the trust boundaries the architecture introduces. No claim is made that BifrostConnect is the only way to implement Part 1's recommendations; several of the compensating controls can be realized with other architectures. Where regulatory wording is interpreted, the interpretation aligns with the guidance issued by Styrelsen for Samfundssikkerhed (SAMSIK) on the Danish NIS2 implementation (Vejledning til NIS 2-loven, June to August 2025).

Cross-references in the form '(Part 1, Scenario X)' point the reader back to the corresponding section of Part 1.

Note on figures and product specifications: text descriptions, figures and architectural diagrams in this guide reflect the target architecture of the BifrostConnect product family. Some components (including AccessGuard and SessionGuard) and some governance patterns (including per-session approval workflows) are deployed where the regulatory regime or operational governance requires them, and may not be present in default deployments. Specific feature availability per plan tier and per release phase is documented separately in current product documentation; reach out to BifrostConnect for the latest availability matrix.

HOW PART 2 MAPS TO PART 1

FIGURE 2. BifrostConnect across the operational lifecycle

One platform, three operational modes, served by one consistent product set.

Bifrost Unit + Manager · DTA / DNA / CTA · AccessGuard · SessionGuard · Secure File Transfers

The same platform serves all three modes.

Figure 2. BifrostConnect across the operational lifecycle. One platform, three modes: prevention, commissioning, and incident response, with a consistent product set across all three.

Part 1 defines four scenarios, a threat model, two complementary architectural lenses (Purdue topology and OT Island direction), and a single operational principle (Zero Standing Privilege). Part 2 is organised around the same structure. The table below shows the mapping.

Part 1 section	Part 2 section	Purpose
Zero Standing Privilege	Zero Standing Privilege with BifrostConnect	Maps the principle to Bifrost session lifecycle
OT Island Principle	OT Island coupling	How Bifrost Unit enforces outbound-only OT posture
Threat model	How BifrostConnect mitigates the threat model	Maps actors, vectors and incidents to Bifrost controls
Scenarios 1 to 4	Scenarios 1 to 4 implementation	Per-scenario product configuration
Comparative summary	Product reference	What each product is and where it applies
Implementation approaches	Co-deployment categories	How Bifrost co-deploys with OT-IDS, SIEM, data diodes
Compliance maturity matrix	Implementation hardening guidance + Architectural transparency	Deployment decisions that deliver Part 1's controls and harden the trust boundaries the architecture introduces

ACCESS TYPE DIFFERENTIATION: KVM VS IP TUNNEL

Part 1 distinguishes two fundamentally different access models. Part 2 uses these consistently throughout:

- **Hardware-based KVM/console access (Direct Native Access):** The operator receives a video stream of the endpoint's display via WebRTC. No network-layer connectivity is established. The operator's device never joins the OT network and has no IP-level access to OT assets. The trust boundary is physical hardware.

- **Session-scoped IP tunnels (Direct Tunnel Access):** The operator's device receives scoped subnet-level IP connectivity to specific endpoints for the session duration. This is temporary network-layer connectivity, tighter than VPN but fundamentally different from KVM. The operator's device can send packets to specified OT endpoints within the tunnel scope.

These are not equivalent security models. KVM provides isolation without network participation. IP tunnels provide scoped network participation with session controls. Both implement Zero Standing Privilege but at different layers. The figure below shows the two trust boundaries in detail.

FIGURE 3. KVM versus IP tunnel access

Two access methods sharing the same identity, time-bound and recording controls.

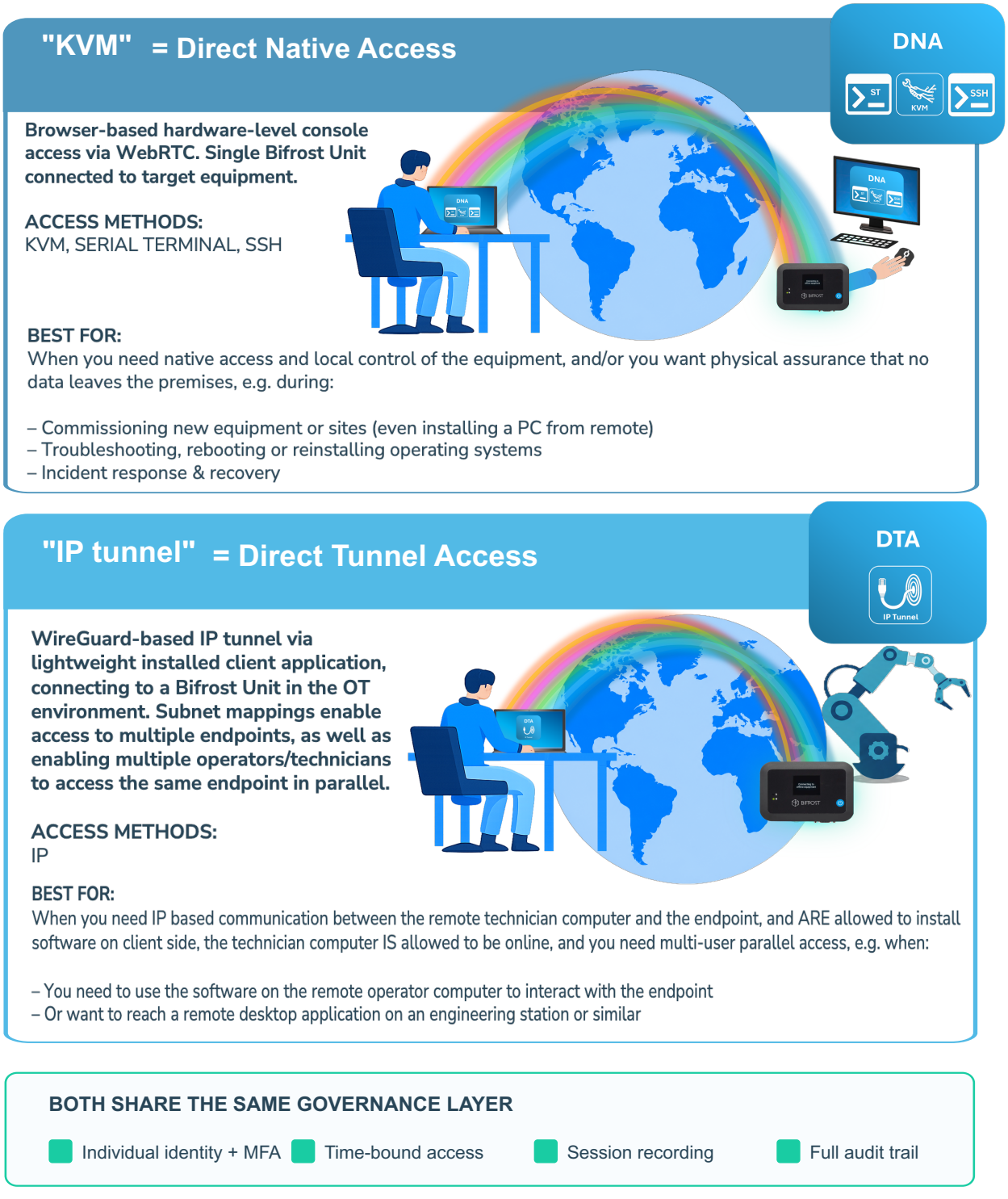


Figure 3. KVM (Direct Native Access) versus IP tunnel (Direct Tunnel Access). Two BifrostConnect access methods sharing the same identity, time-bound and recording controls. Choice depends on whether the endpoint can host an agent.

ZERO STANDING PRIVILEGE WITH BIFROSTCONNECT

Part 1 defines Zero Standing Privilege as 'session-based access, closed by default'. No user should hold a pre-existing, persistent path into the OT network. Access is policy-authorized in advance, opened on session start, used, recorded and torn down, in that order, for every session.

BifrostConnect implements this through administrator-defined access policy in Bifrost Manager (per-user, per-Unit, per-subnet), session-based teardown for Direct Native Access (KVM, SSH, Serial), and time-bound subnet mappings for Direct Tunnel Access (Time-Based Access on Advanced plan and Dedicated Cloud tier). Per-session approval workflows, where a vendor request triggers explicit administrator confirmation before the session opens, are an architectural extension that can be deployed where the regulatory regime or operational governance requires it; the underlying policy engine in Bifrost Manager is designed to support this pattern.

The architecture is realized through the Bifrost Unit's outbound-only posture. The Bifrost Unit maintains only an outbound connection to the BifrostConnect Service on port 443 (WebRTC and MQTT over WSS). No inbound port is open on the OT network. For KVM/console sessions (Direct Native Access), no network-layer connectivity is established at all; the operator sees a video stream without joining the OT network. For IP tunnel sessions (Direct Tunnel Access), scoped subnet-level connectivity is established for the session duration only, with unsolicited inbound traffic blocked by default.

FIGURE 4. Zero Standing Privilege session lifecycle

From a closed default, through an approved, recorded session, back to closed teardown.

1 CLOSED · default

No standing privilege: no tunnel, no open path, no session.
The default state between every engagement.

2 AUTHORIZED

An admin defines the access policy in Bifrost Manager ahead of the session: who, what scope, which window. No live path yet.

3 OPENED

The user authenticates with MFA; the session starts only when it matches the pre-authorized policy. The Bifrost Unit initiates the connection outbound: OT calls out, OT never accepts inbound.

4 ACTIVE

In session: scope enforced and the session recorded. Access is bounded to the approved window and the approved endpoints.

5 CLOSED · teardown

Tunnel destroyed, recording finalized, audit trail complete.
Privilege returns to zero until the next authorized session.

Outbound-only at every stage

The Bifrost Unit always initiates the connection.
No inbound path opens at any point in the lifecycle.

Figure 4. Zero Standing Privilege session lifecycle. Five stages from closed default through approved session back to closed teardown. The Bifrost Unit is always outbound-initiated; no inbound path opens at any stage.

MAPPING TO PART 1'S FIVE PRINCIPLES

Part 1 principle	BifrostConnect implementation
1. Zero Standing Privilege	No access exists between sessions. Direct Native Access and Direct Tunnel Access sessions terminate when the browser session ends (no persistent tunnel); Direct Tunnel Access subnet mappings can be configured time-bound (Advanced plan / Dedicated Cloud tier). Bifrost Manager enforces JIT access windows; AccessGuard is designed to enforce mandatory TOTP per session at the engineering station.
2. The OT Island Principle	The Bifrost Unit initiates outbound connections only and listens on no inbound port (outbound 443 only): OT calls out, OT never accepts inbound. For KVM (Direct Native Access) there is no network-layer connectivity at all; IP-tunnel connectivity is scoped to specific endpoints for the session only.
3. Defence in depth	Independent layers wrap the asset: individual identity and MFA (Bifrost Manager via Auth0; AccessGuard TOTP at the station), per-session approval and JIT, scoped network path (masquerading, subnet scoping), session mediation through the Bifrost Unit, session recording (AccessGuard H.264 with DPAPI; SessionGuard WebRTC to a customer VM where deployed), and one-way log export to SIEM (optionally via a data diode).
4. Minimum viable controls scale to context	The same control gates apply to every scenario; implementation depth scales with site maturity. Each scenario carries a documented minimum-viable floor and a target-state ceiling (see the per-scenario capability tables).
5. Verification over assumption	Every control above is acceptance-testable and anchored to BifrostConnect Security Documentation; session recordings and audit logs are the evidence that each control operated as designed during the access window.

OT ISLAND COUPLING

Part 1 introduces the OT Island Principle as a directional complement to Purdue: OT calls out, OT never receives. Architecturally, BifrostConnect implements this principle: the Bifrost Unit initiates outbound connections to the BifrostConnect Service; it accepts no inbound connections. The OT environment remains an island. The Bifrost Unit is the enforcement point of the outbound-only principle at the OT boundary.

The outbound-only posture does not by itself require hardware: a software agent can also be outbound-initiated. The Bifrost Unit exists as dedicated hardware for the trust properties a software agent running on a customer-managed OT host cannot guarantee. Its SoC secure-boot fuses are burnt at manufacture and are non-reversible, so it cannot boot alternative firmware; it runs a stripped industrial Linux with no local users, no SSH, no local web services, and no physical service or debugging ports; firmware updates are signed and delivered over-the-air only; and its battery and built-in LTE provide an out-of-band path independent of the customer network. A general-purpose

host running a software agent inherits that host's users, services, patch state, and exploitable surface; the dedicated Unit does not.

HOW BIFROSTCONNECT MITIGATES PART 1'S THREAT MODEL

Part 1 identifies a threat model consisting of named threat actors, attack vectors and reference incidents. This section maps each to the control layer in BifrostConnect that addresses it.

THREAT ACTORS

Part 1 names five classes of threat actor relevant to OT third-party access. Nation-state APTs (e.g. Volt Typhoon, Sandworm) pursue strategic pre-positioning in critical infrastructure. Ransomware operators monetise disruption and exfiltration. Hacktivists target utilities for political messaging. Malicious insiders abuse authorised access. Supply-chain attackers weaponise the vendor relationship itself.

Threat actor (Part 1)	How BifrostConnect reduces the remote-access attack surface for this actor
Nation-state actors (e.g. Volt Typhoon, Sandworm)	Removes the always-on remote-access tunnel that LOTL-style intrusions reuse. Hardware trust boundary, no local web services, signed firmware only, OTA-only updates, and non-reversible fuse-enforced secure boot reduce the Unit's own exploitable surface. Does not address SOHO-router compromise, spear-phishing, or other entry vectors these actors are known to use.
Ransomware groups targeting OT (e.g. ALPHV/BlackCat)	Closes the always-on remote-access path that ransomware operators have used to reach OT (Colonial Pipeline pattern). No persistent tunnel, no broad network access, session-based teardown. SessionGuard provides post-incident reconstruction when deployed and active. Does not address phishing, IT-side compromise, or backup destruction; ransomware response requires a complete IR programme.
Insider threat (authorised user acting beyond scope)	Individual identity (no shared accounts), session recording where SessionGuard or AccessGuard is deployed, SIEM forwarding (Dedicated Cloud tier), JIT time-boxing, and least-privilege role model in Bifrost Manager raise the cost and traceability of insider misuse during the approved session window. Does not prevent misuse during a legitimately approved session; that residual risk is addressed in the Part 1 residual-risk section through procedural controls.

Threat actor (Part 1)	How BifrostConnect reduces the remote-access attack surface for this actor
Compromised vendor (supply chain)	Physical broker isolates vendor PC from OT network. For KVM sessions, vendor PC has no network access to OT at all. For IP tunnel sessions, vendor PC IP never appears on the OT LAN; masquerading enforces address translation. Does not address compromise inside the vendor session itself (e.g. malicious code already present on the vendor laptop being executed during a legitimate session); SessionGuard recording supports detection and forensics, not prevention.
Opportunistic external scanner	Endpoints never exposed to the internet; endpoint IP addresses hidden; port scans through Bifrost interface are impossible because no inbound port is open.

ATTACK VECTORS

The attack vectors that recur across published OT incidents cluster into five patterns: exposed remote access (VPN or RDP left reachable), credential theft and reuse, supply-chain compromise via vendor tooling, unpatched OT endpoints exploited through living-off-the-land techniques, and shared bastion or jump hosts that become persistent footholds. Each vector is addressed below.

Attack vector (Part 1)	Bifrost mitigation
Credential theft / reuse	Mandatory MFA (Auth0); TOTP tied to the Bifrost Unit in attended mode; no credentials pass through the Bifrost Service in the clear.
Lateral movement from vendor PC	For KVM: no network-layer connectivity exists. For IP tunnels: operator PC does not receive a local IP on the OT network - masquerading translates source addresses. Subnet mappings are scoped to specific endpoints.
Persistent access paths / forgotten tunnels	Direct Native Access sessions terminate on browser close; Direct Tunnel Access subnet mappings can be configured as time-bound on the Advanced plan and Dedicated Cloud tier. No standing IP path exists by default.
Man-in-the-middle on transport	TLS for signalling, DTLS-SRTP end-to-end for WebRTC, WireGuard encryption for Direct Tunnel; private keys never leave the client.
Living-off-the-Land techniques in OT	Session recording captures all vendor tool usage regardless of whether the tool is 'legitimate'. Protocol-level detection requires OT-IDS co-deployment (see Co-deployment categories).
Untracked vendor software on OT station	AccessGuard is designed to scope which applications the vendor can launch; session video captures all activity regardless of application.

REFERENCE INCIDENTS

Five publicly documented incidents illustrate the failure modes that Part 1's framework is designed to prevent: Colonial Pipeline (2021, exposed credential on a legacy VPN); TRITON / TRISIS (2017, safety-system compromise via engineering workstation); Oldsmar water treatment (2021, attribution disputed, shared TeamViewer credential); Ukrainian grid (2015, BlackEnergy against utilities via

phishing and VPN abuse); and the Danish energy-sector campaign (SektorCERT, attacks May 2023, public report November 2023; 22 energy companies impacted across two waves via Zyxel firewall vulnerabilities, CVE-2023-28771 and the zero-days CVE-2023-33009 and CVE-2023-33010). Part 1 highlights three of these (Colonial Pipeline, the SektorCERT campaign, and TRITON / TRISIS) as its core reference incidents; Part 2 expands the set to five to cover the failure modes most often raised in OT procurement and audit reviews.

Incident class (Part 1)	What Bifrost would have constrained
Oldsmar, Florida (2021, attribution disputed)	Individual accounts, MFA, closed-by-default, session video would have given a named operator, a recording, and a bounded window - none of which existed.
Pipeline incident via exposed credentials	No persistent credential path; sessions require TOTP; SIEM export would have flagged anomalous authentication attempts in real time.
Supply chain malware via vendor laptop	For KVM sessions: vendor PC never has network access to OT assets. For IP tunnel sessions: vendor PC IP never appears on the OT network.
Engineering station compromise via shared admin password	AccessGuard is designed to enforce individual accounts and mandatory MFA; the architecture is designed so shared admin credentials cannot be configured.
Danish energy sector attack (2023, 22 companies via firewall vulnerabilities)	Bifrost Unit does not require inbound firewall rules on the OT network. The attack exploited exposed firewall management interfaces; the Bifrost Unit exposes none.

SCENARIO IMPLEMENTATION OVERVIEW

Part 1 defines four scenarios derived from two axes: where the programming software is located (engineering station vs vendor PC) and the scale of the OT operation (small with no SOC vs large with SOC, PAM, SIEM). Each scenario maps to a specific BifrostConnect product mix. The figure below shows the four implementations side by side. The detailed configuration for each scenario follows in the next four sections.

FIGURE 5. Four OT access scenarios on one architecture

Two axes, four patterns. Each quadrant shows the BifrostConnect product mix for that scenario.

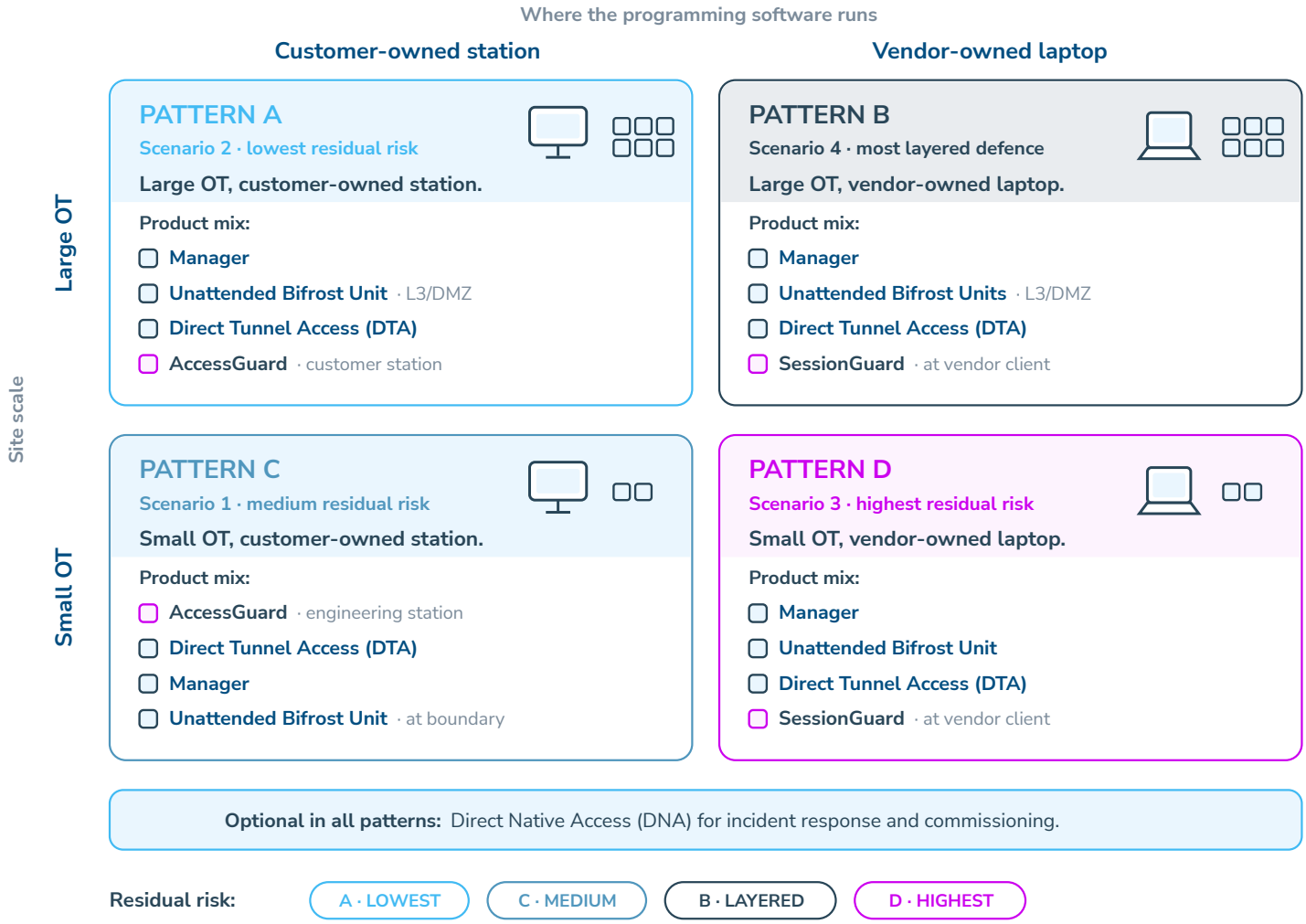
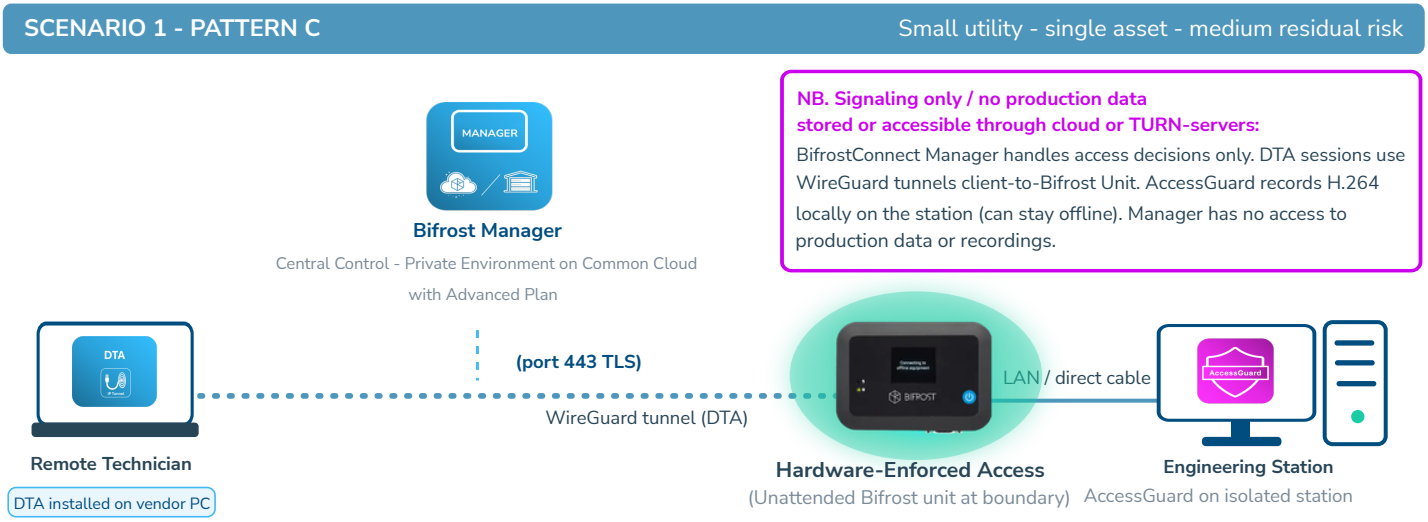


Figure 5. Four OT access scenarios on one architecture. Two axes (OT scale and tooling location) define four scenarios. The five shared principles apply to all four. Product mix varies by scenario.

SCENARIO 1 IMPLEMENTATION: SMALL OT, SOFTWARE ON STATION (PATTERN C)

SCENARIO 1. Implementation - Pattern C

Small OT, software on customer station. AccessGuard primary, with a recommended Unattended Bifrost Unit at the boundary.



SCENARIO 1 PRODUCT MIX

- AccessGuard (primary) - mini-PAM on engineering station, localhost-only 127.0.0.1:7531
- Direct Tunnel Access (DTA) - lightweight client on vendor PC, WireGuard to Bifrost Unit
- Bifrost Manager - access decisions, MFA, audit logging
- Recommended: Unattended Bifrost Unit at the boundary
- H.264 recording stored locally with DPAPI encryption

COMPLIANCE EVIDENCE

- NIS2 Art. 21(2)(d), (i), (j) - access control + supplier risk
- BEK 260 §§29-32 supplier procedures + remote-access procedures
- BEK 260 §§51-53 and §55 stk. - identification + auth
- IEC 62443-3-3:2019 SR 1.1 + SR 2.1 + SR 2.6
- Mandatory TOTP enrolment per vendor technician account

Scenario 1 implementation. Software on engineering station, small OT environment, single asset. Vendor uses tools already installed on the station; AccessGuard is designed to enforce local control while the Bifrost Unit provides outbound-only WireGuard tunnelling. Smallest possible footprint, tightest possible scope.

Primary products: the canonical Scenario 1 stack (Direct Tunnel Access + AccessGuard + Bifrost Manager + an unattended Bifrost Unit at the boundary). AccessGuard alone, running on the site's existing remote-access path, is the minimum-viable floor that closes the audit gap for the smallest sites.

Cross-reference: Part 1, Scenario 1 / Pattern C.

PART 1 REQUIREMENT RECAP

Small utility, two IT staff, standalone engineering station with PLC programming software. Vendor needs screen-level access. No AD, no server infrastructure, no security staff. Security must be architectural.

BIFROSTCONNECT IMPLEMENTATION

Minimum-viable floor: AccessGuard, installed directly on the engineering station and reached over the site's existing remote-access path. The configuration below details this floor; the canonical best-practice target adds an unattended Bifrost Unit at the boundary (see Recommended hardening, below).

Configuration:

- AccessGuard agent installed on the Windows engineering station (Windows XP SP3+ to Windows 11 (incl. Server 2003+), 2 GB RAM free, port 7531).
- Localhost-only binding (127.0.0.1:7531). No network exposure of the agent.
- Mandatory TOTP enrolment for every vendor technician account. TOTP cannot be disabled.
- Application launch scope: only the programming software the vendor needs. No general shell or Explorer access.
- H.264 session recording enabled by default. Recordings encrypted at rest using Windows DPAPI.
- Recordings stored locally on the OT network. No cloud dependency.
- Time-window configured per vendor engagement. Access expires automatically at the end of the window.

COMPLIANCE EVIDENCE MAPPING (PART 1, SCENARIO 1 REGULATORY ALIGNMENT)

Requirement (source)	Technical evidence BifrostConnect provides	Organisational control still required
NIS2 Art. 21(2)(d): supply chain security	Audit trail of all vendor sessions with individual identity, MFA proof, H.264 session recording.	Vendor contractual obligations, supplier risk assessment, incident notification clauses, regular access reviews.
NIS2 Art. 21(2)(i): access control for privileged access	Per-vendor accounts in AccessGuard with mandatory TOTP; application-scoped access.	Access control policy document, periodic review, process for revoking access when vendor relationship ends.
NIS2 Art. 21(2)(j): MFA where appropriate	Mandatory TOTP on every AccessGuard session (cannot be disabled).	Risk assessment documenting where MFA is proportionate (NIS2 requires assessment, not blanket MFA).

Requirement (source)	Technical evidence BifrostConnect provides	Organisational control still required
Danish NIS2 Act §6: identity-bound, MFA; BEK 260 §55 stk. 2 time-limited, §§64-67 logged	Individual accounts, TOTP, time-windowed access, DPAPI-encrypted session recordings.	Written access control policy, staff awareness of vendor session governance.
IEC 62443-2-4:2024[1] SP.07 Remote access (BR.01-04)	Session recording, authentication events, scoped application access.	Supplier qualification process, documented security requirements for vendors.
BEK 260 §§51-53 and §55 stk. 2: remote access identity, MFA, time-bound	AccessGuard TOTP, individual identity, time-window configuration.	Written remote access policy, training of operations staff on vendor session procedures.

IMPLEMENTATION REQUIREMENTS FOR SCENARIO 1

Deploy AccessGuard with the following operational decisions in mind so the control envelope is what is documented in compliance evidence:

- Network connectivity: AccessGuard is designed to reach the engineering station over the OT network. For fully air-gapped stations, plan vendor work either on-site or via a Bifrost Unit out-of-band path (see Scenario 3) - both produce equivalent recording and identity evidence.

- Delivery channel discipline: AccessGuard is the only authorised vendor delivery path. KVM switches, TeamViewer and AnyDesk are out of scope; remove or block them as part of the access policy so the recorded path is the only path.

- Station-level vs network-level isolation: AccessGuard is the application-and-recording control on the station. Pair it with a station-level network segmentation (VLAN or local firewall) so a compromised station cannot reach other OT assets. The two controls together close the boundary.

[1] DS/EN IEC 62443-2-4:2024. Single user license, BifrostConnect ApS, retrieved 2026-05-04.

RECOMMENDED HARDENING:

ADD A BIFROST UNIT AT THE BOUNDARY

Where AccessGuard is paired with an existing remote-access path, it delivers the Scenario 1 minimum viable control envelope as a compensating posture. For organisations that want a stronger boundary - for example sites that handle drinking water, district heating, or other critical infrastructure where the regulator looks for hardware-enforced segmentation - adding an unattended Bifrost Unit at the boundary of the engineering station's network is the recommended next step (the canonical Scenario 1 best-practice combination). The Unit gives you outbound-only OT posture, an out-of-band 4G/LTE access path for incident response, and the option to add SessionGuard recording later without re-architecting.

The canonical Scenario 1 best-practice combination is Direct Tunnel Access + AccessGuard + Bifrost Manager + an unattended Bifrost Unit at the boundary. AccessGuard with disciplined operational controls and an existing remote-access path satisfies NIS2 Art. 21(2)(d), (i), (j); BEK 260 §§29-32 (supplier procedures and remote-access procedures for direct suppliers); and BEK 260 §§51-53 and §55 stk. 2 (access control, MFA, time-bounded remote access) as a compensating posture; the full combination is the recommended target.

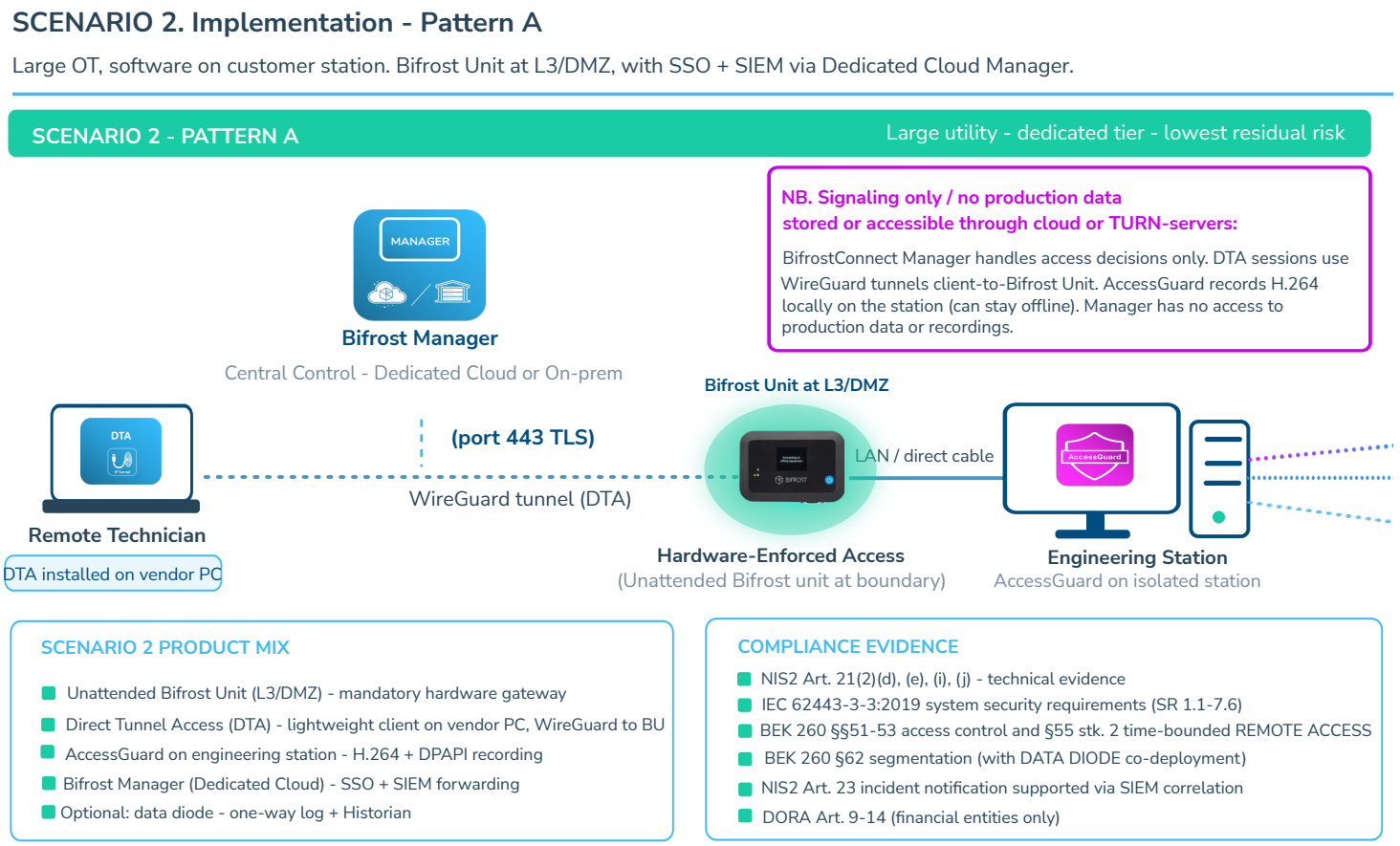
MATURITY PROFILE:

MINIMUM VIABLE VS TARGET STATE (SCENARIO 1)

The table below distinguishes the floor (what the guide treats as required) from the ceiling (what mature deployments aim for). Read the guide's recommendations as a floor, not a ceiling: hitting minimum viable closes the audit gap; reaching target state is the operationally-resilient deployment.

Capability	Minimum viable (Scenario 1 floor)	Target state (Scenario 1 ceiling)
Identity	Per-vendor account in AccessGuard, mandatory TOTP per session.	Federated to enterprise IdP via Bifrost Manager (Dedicated Cloud / on-premises tier).
Recording	AccessGuard H.264 + DPAPI on the station, customer-controlled storage.	AccessGuard plus SessionGuard cross-check on a separate VM for evidence-chain redundancy.
Network boundary	Station-level VLAN or local firewall isolating the engineering station.	Bifrost Unit at the boundary - outbound-only OT posture, 4G/LTE out-of-band path for incident response.
Audit + monitoring	Local audit log on the station, periodic export to a SIEM.	Bifrost Manager native SIEM forwarding (Dedicated Cloud tier) plus OT-IDS co-deployment for protocol-level alerting.

SCENARIO 2 IMPLEMENTATION: LARGE OT, SOFTWARE ON STATION (PATTERN A)



Scenario 2 implementation. Software on engineering station, large OT environment, layered network. Bifrost Unit at L3/DMZ with an optional data diode for one-way log and file flow out of OT zones.

Primary products: Bifrost Unit (unattended), AccessGuard, Direct Tunnel Access, Bifrost Manager
Cross-reference: Part 1, Scenario 2 / Pattern A.

PART 1 REQUIREMENT RECAP

Large utility or industrial site with dedicated OT security staff, existing SOC, PAM, SIEM. Programming software is installed on engineering stations under operations control. Vendor access must integrate with enterprise identity, be logged to SIEM and support fast emergency access.

BIFROSTCONNECT IMPLEMENTATION

Primary products: Unattended Bifrost Units + Direct Tunnel Access + AccessGuard + Bifrost Manager. Enterprise SSO, RBAC, JIT access windows and SIEM forwarding are delivered on the Dedicated Cloud / on-premises tier. Direct Native Access remains available for screen-level commissioning and incident response where IP-layer access is unnecessary.

Configuration:

- Bifrost Manager deployed on BifrostConnect Dedicated Cloud or on-premises (required for SSO and SIEM).
- SSO configured against the customer's existing IdP (SAML, OAuth2, AD or LDAP).
- Vendor groups defined with Just-in-Time (JIT) time-boxed access windows.
- AccessGuard deployed on engineering stations; account provisioning flows from the Bifrost Manager identity layer.
- SIEM integration configured to forward authentication events, access grants and denials, session start and end, and recording metadata.
- Audit logging enabled for all Manager actions, including admin operations.
- Firmware updates on Bifrost Units managed via OTA from Bifrost Manager with session-aware postponement.

COMPLIANCE EVIDENCE MAPPING (PART 1, SCENARIO 2 REGULATORY ALIGNMENT)

Requirement (source)	Technical evidence BifrostConnect provides	Organisational control still required
NIS2 Art. 21(2)(b): incident handling	Session recordings, audit logs, SIEM-forwarded events for forensic investigation and 24h/72h/1-month staged reporting.	Incident response plan, trained incident response team, established communication with competent authority, legal counsel on standby.
NIS2 Art. 21(2)(c): business continuity	Session logs for disaster recovery verification, attended Bifrost Unit for emergency access.	Business continuity plan, tested failover procedures, documented recovery priorities.
NIS2 Art. 21(2)(d): supply chain security	JIT access, SSO-federated vendor identity, per-vendor group scoping, session recording, SIEM export.	Vendor contractual obligations, regular vendor access reviews, supplier risk assessment, incident notification clauses.

Requirement (source)	Technical evidence BifrostConnect provides	Organisational control still required
NIS2 Art. 23: 24h/72h/1-month staged reporting	SIEM-integrated session logs for scope determination within reporting deadline.	Established notification workflow, legal review of reporting obligations, designated incident contact.
BEK 260 §62: network segmentation during vendor access	Bifrost Unit as boundary device, outbound-only posture, masquerading.	Network architecture documentation, segmentation verification testing.
IEC 62443-3-3:2019[2] FR 5 Restricted data flow (zone isolation)	Hardware-enforced access boundary between enterprise and OT zones.	Security level assignments per zone, conduit documentation, periodic architecture review.

IMPLEMENTATION REQUIREMENTS FOR SCENARIO 2

Confirm the following operational decisions before go-live so the deployment delivers the SSO, audit and recording properties the compliance evidence will rely on:

- Deployment tier: enterprise SSO and SIEM forwarding are delivered on BifrostConnect Dedicated Cloud or on-premises Manager. Procure the right tier at the start so the SSO trust and audit chain are established before the first vendor session.

- Recording verification: include the SessionGuard or AccessGuard acceptance test in rollout (see Implementation hardening guidance). Treat the test as a go-live gate so recording is provably enforced from day one.

- PAM co-deployment: keep your existing PAM platform for credential vaulting. BifrostConnect provides the access-and-audit layer upstream of credentials; mapping which control owns what avoids overlap and keeps the credential rotation policy in PAM where the auditor expects it.

[2] DS/EN IEC 62443-3-3:2019. Single user license, BifrostConnect ApS, retrieved 2026-05-04.

OPTIONAL CO-DEPLOYMENT:

CERTIFIED DATA DIODE

For Scenario 2 sites that operate Historian replication into the IT analytics stack, or that need to forward OT logs into a centralised SIEM without opening a return path into the OT zone, a certified data diode is the recommended unidirectional transport. The diode is co-deployed alongside BifrostConnect rather than replacing any of its functions:

- One-way log export: place the diode between the OT logging infrastructure and the enterprise SIEM destination. Bifrost Manager events flow to SIEM through the standard outbound channel; OT-IDS alerts and asset telemetry flow through the diode. Both meet at the SIEM for correlation.

- One-way Historian replication: deploy one-way database replication on the diode for replicating the Historian (or any OPC UA / SQL data store) to the IT analytics stack without an inbound IT-to-OT path.

- Inline file scanning for vendor uploads: chain a data-diode file security gateway (multi-engine scan, content disarm/reconstruction) ahead of Direct Tunnel Access file uploads so vendor-introduced files are sanitised before they touch the OT zone.

These are co-deployments, not replacements: the diode handles unidirectional transport; BifrostConnect handles the human-session governance. Both forward to the customer SIEM.

MATURITY PROFILE:

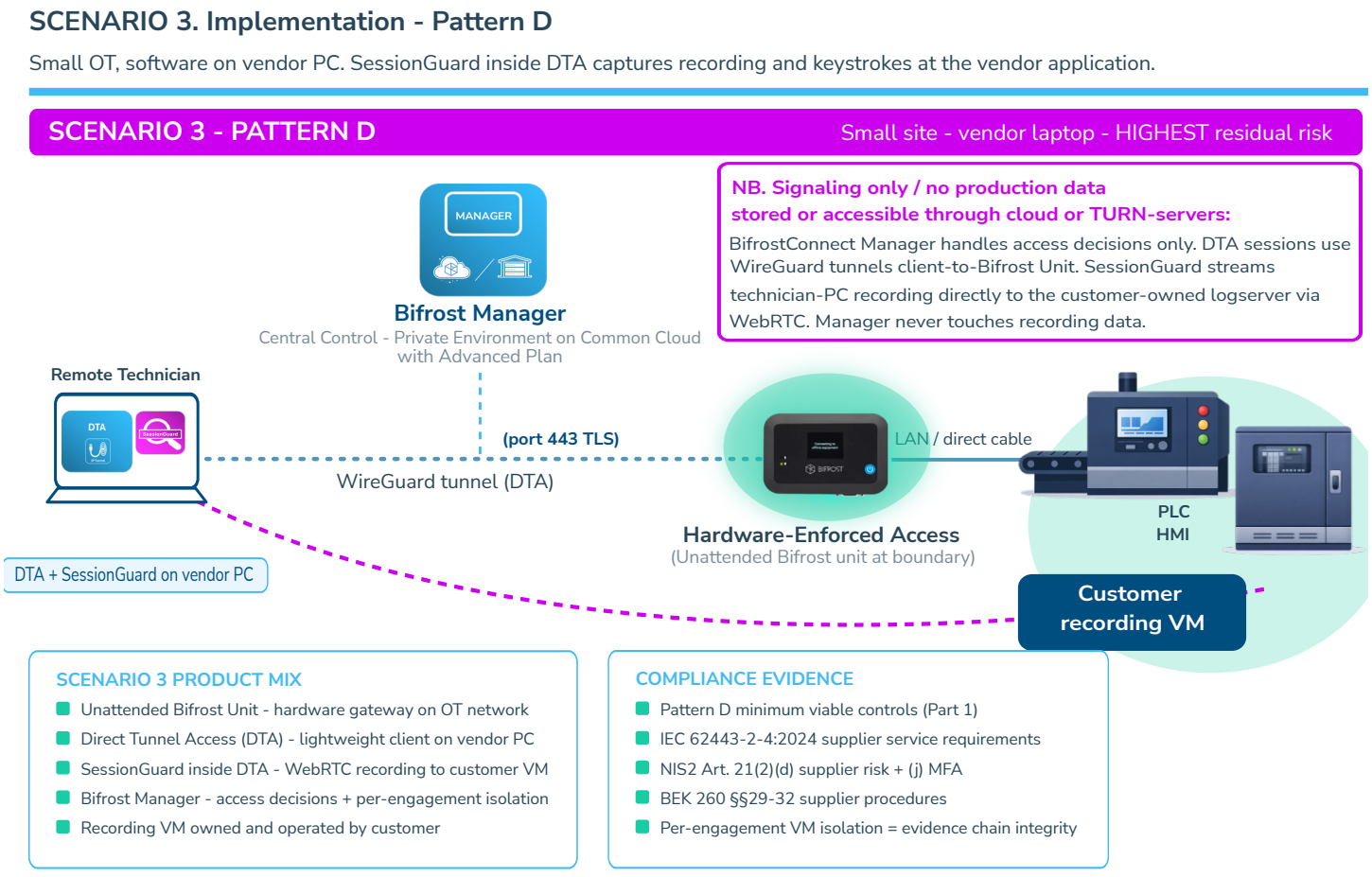
MINIMUM VIABLE VS TARGET STATE (SCENARIO 2)

Read the guide's recommendations as a floor, not a ceiling. Minimum viable closes the compliance gap for a large OT site; target state adds resilience, redundancy, and diode-protected one-way transport.

Capability	Minimum viable (Scenario 2 floor)	Target state (Scenario 2 ceiling)
Identity	Bifrost Manager with Auth0 MFA on admin accounts; per-vendor accounts.	Enterprise SSO via SAML / OAuth 2.0 / AD / LDAP (Dedicated Cloud / on-premises tier); conditional access and hardware-token MFA on admin sign-in (delivered through the customer's federated IdP).
Recording	AccessGuard on engineering stations (H.264 + DPAPI).	AccessGuard + SessionGuard for cross-check; tamper alerts forwarded to SOC.

Capability	Minimum viable (Scenario 2 floor)	Target state (Scenario 2 ceiling)
Network boundary	Bifrost Unit at OT boundary, outbound-only on port 443.	Bifrost Unit + a certified data diode for one-way log export and Historian replication.
Audit + monitoring	Native SIEM forwarding from Bifrost Manager (Dedicated Cloud tier).	Bifrost Manager + OT-IDS co-deployment correlated at the SIEM.
Vendor file handling	Vendor-supplied files reviewed by ops before deployment.	Inline data-diode file security gateway (multi-engine malware scanning + content disarm/reconstruction) on every Direct Tunnel Access file upload.

SCENARIO 3 IMPLEMENTATION:
SMALL OT, VENDOR PC (PATTERN D)



Scenario 3 implementation. Vendor brings own laptop or VM with full toolchain into a small OT environment. SessionGuard inside DTA is designed to capture recording and keystrokes at the vendor application. No software footprint on the OT station.

Primary products: Bifrost Unit (unattended), Direct Tunnel Access, SessionGuard, Bifrost Manager

Cross-reference: Part 1, Scenario 3 / Pattern D.

PART 1 REQUIREMENT RECAP

Small utility, software licensed on the vendor technician's own PC (common for Danish water sector). The vendor travels to the site with their own laptop and connects it to the OT network. Part 1 identifies this as the highest proportional risk: an uncontrolled device in direct contact with PLCs, with no enterprise IT to harden it.

BIFROSTCONNECT IMPLEMENTATION

Primary products: Unattended Bifrost Unit + Direct Tunnel Access + SessionGuard (enforced session recording to a customer-controlled log server when deployed per the hardening guidance) + Bifrost Manager. The SessionGuard recording engine is designed to be packaged with the Direct Tunnel Access client and must be installed on the technician PC.

Configuration:

- Bifrost Unit deployed on the OT network as the access gateway. Unattended variant is the canonical default (admin-initiated session via Manager + MFA + mobile-app verification); the attended variant is selected where on-site personnel must physically authorise each session via the Unit's TOTP button.

- Bifrost Unit maintains outbound-only connection to BifrostConnect Service on port 443 (4G or WAN). OT Island principle enforced: outbound only, no inbound port open.

- Vendor PC connects via Direct Tunnel Access (WireGuard tunnel, scoped to specific subnet/IP) or Direct Native Access (browser KVM, no network-layer connectivity). The choice determines the security profile.

    - **Direct Native Access (KVM):** vendor PC has zero network access to OT assets. Video stream only. Highest isolation.

    - **Direct Tunnel Access:** vendor PC gets scoped, temporary IP connectivity. Necessary when vendor software must send IP traffic to PLC. Lower isolation than Direct Native Access but still session-scoped and recorded.

- SessionGuard is designed to deploy on a customer-owned recording VM per vendor engagement. WebRTC screen capture and keystroke logging flow directly from the vendor operator console to the customer's VM by design.

- Physical masquerading on the Bifrost Unit ensures only the Unit's IP is visible to OT equipment.

- TOTP button on the attended Unit enforces on-site consent for every session.

COMPLIANCE EVIDENCE MAPPING (PART 1, SCENARIO 3 REGULATORY ALIGNMENT)

Requirement (source)	Technical evidence BifrostConnect provides	Organisational control still required
NIS2 Art. 21(2)(d): supply chain (vendor PC on OT network)	Bifrost Unit prevents vendor PC from joining OT network (KVM) or constrains access to scoped tunnel (Direct Tunnel). Individual identity captured.	Vendor device security requirements in contract, self-certification or attestation of device compliance, defined maintenance procedure.
NIS2 Art. 21(2)(e): security in network maintenance	Session recording of all maintenance activity, time-bounded access windows.	Change request documentation (even a logged email approval for small orgs), post-maintenance verification by operations.
NIS2 Art. 21(2)(i): access control for vendor device access	Gateway-level authentication, TOTP, individual identity, scoped network access.	Written vendor access policy, process for vendor de-provisioning when contract ends.
IEC 62443-2-4:2024 SP.07 Remote access + SP.01 Solution staffing	Bifrost Manager identity, SessionGuard recording, time-limited session.	Technician qualification verification, documented scope per maintenance task.
BEK 260 §§51-53: only authorised endpoints on OT	Bifrost Unit broker - vendor PC never directly on OT LAN (KVM) or scoped-only (Direct Tunnel).	Written endpoint authorisation policy, physical access procedures for on-site maintenance.

IMPLEMENTATION REQUIREMENTS FOR SCENARIO 3

Scenario 3 is the highest-risk quadrant by Part 1's analysis (vendor PC, small OT). The following deployment decisions make the BifrostConnect control envelope hold:

- Recording layer ownership: SessionGuard is designed to capture the operator's screen and keystrokes. Pair it with OT-IDS co-deployment when protocol-level evidence on Modbus / OPC UA / S7comm is also required - the two recordings together produce the complete forensic chain.

- Recording VM as a deployment dependency: SessionGuard is designed to run on a customer-deployed VM per engagement. Schedule the VM build, ownership and patch responsibility before the first vendor session. The recording claim is real once the VM is in place.

- Acceptance test as a go-live gate: validate three properties before the first production session: (a) the session cannot start when the recording VM is unreachable, (b) recordings land in customer-

controlled storage, (c) tampering alerts reach the SOC. Document the test result in the rollout runbook.

- Operator-side platform: deploy the Direct Tunnel Access client (installed lightweight client on macOS / Windows; supports multi-user parallel access and subnet mapping). Match the deployment to the vendor's tooling rather than retrofitting later.

- Access model selection: when KVM (Direct Native Access) covers the vendor's task, use it - the vendor PC then has zero IP path to OT. Reserve Direct Tunnel Access for tasks that genuinely need IP-level interaction (e.g. firmware uploads, multi-port debug). Documenting the choice per task closes the audit trail.

MATURITY PROFILE:
MINIMUM VIABLE VS TARGET STATE (SCENARIO 3)

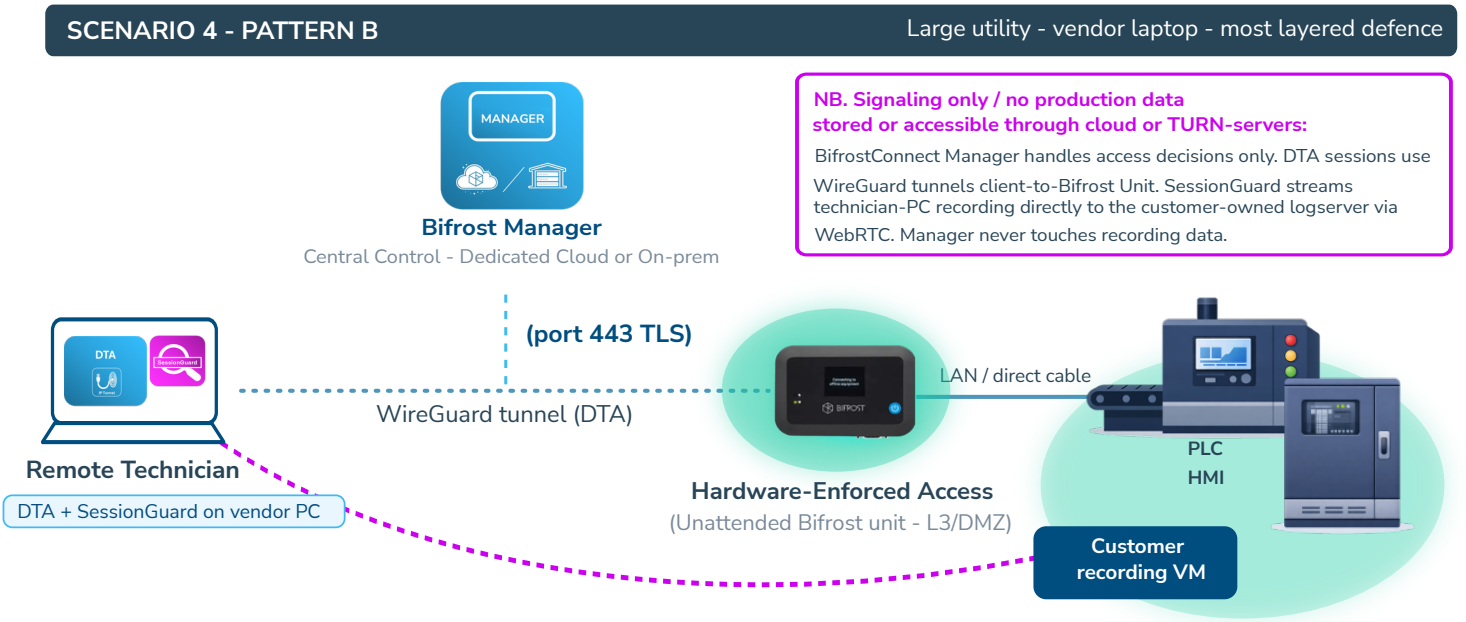
Scenario 3 is Part 1's highest-risk quadrant. Minimum viable closes the BEK 260 §§29-32 (supplier procedures), §§51-53 and §55 stk. 2 and NIS2 supply-chain gap; target state adds the depth needed for sites where the regulator will examine the deployment after an incident.

Capability	Minimum viable (Scenario 3 floor)	Target state (Scenario 3 ceiling)
Identity	Unattended Bifrost Unit (canonical default) with attended variant available where on-site authorisation is required; per-vendor accounts in Bifrost Manager.	Federated SSO via Bifrost Manager Dedicated Cloud / on-premises tier; conditional access on admin sign-in (delivered through the customer's federated IdP).
Recording	SessionGuard on a customer-deployed VM per engagement (the recording floor).	SessionGuard plus OT-IDS packet capture for protocol-level evidence; tamper alerts to SOC.
Network boundary	Bifrost Unit (unattended canonical, attended variant where required), outbound-only, masquerading active.	Bifrost Unit attended + 4G/LTE out-of-band + scheduled time-bound Direct Tunnel Access (Advanced plan or Dedicated Cloud tier).
Vendor PC trust	Vendor PC connects via attended session, scoped to specific endpoints.	Direct Native Access preferred over Direct Tunnel Access where the task allows; access model documented per task.
Audit + monitoring	Audit via the Manager/Service; SIEM forwarding (Dedicated Cloud tier).	Manager + OT-IDS + diode-protected unidirectional log export to enterprise SIEM.

SCENARIO 4 IMPLEMENTATION:
LARGE OT, VENDOR PC (PATTERN B)

SCENARIO 4. Implementation - Pattern B

Large OT, software on vendor PC. Bifrost Unit at L3/DMZ + DTA + SessionGuard + optional OT-IDS + optional data diode.



SCENARIO 4 PRODUCT MIX

- Unattended Bifrost Unit (L3/DMZ) at vendor access point
- Direct Tunnel Access (DTA) - WireGuard via vendor PC
- SessionGuard inside DTA - per-engagement recording VM
- Bifrost Manager (Dedicated Cloud) - SSO + SIEM
- Optional: OT-IDS for DPI
- Optional: data diode - one-way log export

COMPLIANCE EVIDENCE

- NIS2 Art. 21(2)(d), (e), (i), (j) - technical evidence
- IEC 62443-3-3:2019 + IEC 62443-2-4:2024 supplier requirements
- BEK 260 §§51-62 (access control + segmentation)
- NAC + vendor-DMZ contain untrusted vendor device
- OT-IDS alerts correlated at SIEM with Manager audit log
- DORA Art. 9-14 + 28 (financial entities only)

Scenario 4 implementation. Vendor brings own laptop or VM with full toolchain into a large OT environment. Layered deployment with Bifrost Unit at L3/DMZ, vendor session contained in DTA and SessionGuard, optional diode for log export.

Primary products: Bifrost Unit (unattended at L3 / DMZ), Direct Tunnel Access, SessionGuard, Bifrost Manager, with optional co-deployment of an OT-IDS and a certified data diode.

Cross-reference: Part 1, Scenario 4 / Pattern B.

PART 1 REQUIREMENT RECAP

Large utility or industrial site with vendor-owned licensed software on vendor laptops. Part 1 requires layered controls: NAC, vendor DMZ, OT-IDS with deep packet inspection, protocol-level monitoring, centralised SIEM, and isolation between vendor engagements.

BIFROSTCONNECT IMPLEMENTATION

Primary products: Unattended Bifrost Units + Direct Tunnel Access + SessionGuard (enforced session recording to a customer-controlled log server when deployed per the hardening guidance) + Bifrost Manager (RBAC, JIT, audit). SIEM forwarding is delivered on the Dedicated Cloud / on-premises tier. The SessionGuard recording engine is designed to be packaged with the Direct Tunnel Access client. Optional co-deployment of OT-IDS for protocol-level deep packet inspection and a data diode for one-way log export and Historian replication.

Configuration:

- Bifrost Units deployed at each vendor access point on the OT network (Purdue L3 / DMZ).
- Unattended variant used for operations requiring admin-driven access without on-site presence.
- Bifrost Manager hosted on Dedicated Cloud or on-premises; SSO federated to enterprise IdP.
- SessionGuard VM deployed per customer engagement, giving isolation between different vendor-customer relationships.
- An OT-IDS co-deployed on the OT network to provide deep packet inspection on actual OT protocols (Modbus TCP, OPC UA, S7comm, IEC-104). This is co-deployment, not API-level integration: BifrostConnect and OT-IDS operate independently, correlated at the SIEM layer.
- SIEM receives: Bifrost Manager events, OT-IDS alerts, SessionGuard recording metadata. Correlation happens in the SIEM, not in BifrostConnect.
- A certified data diode is available for unidirectional log export or unidirectional Historian replication as a compensating control where required.

COMPLIANCE EVIDENCE MAPPING (PART 1, SCENARIO 4 REGULATORY ALIGNMENT)

Requirement (source)	Technical evidence BifrostConnect provides	Organizational control still required
NIS2 Art. 21(2)(d): supply chain (vendor device on OT)	JIT access, SSO-federated vendor identity, SessionGuard recording, Bifrost Unit network isolation, SIEM export.	Vendor device compliance verification (NAC health check), background checks for critical infrastructure, vendor contracts.
NIS2 Art. 23: 24h/72h/1-month staged reporting	Comprehensive session logs, SIEM-integrated audit trail, SessionGuard recordings for scope determination.	Incident response plan with 24/72-hour workflow, trained reporting team, legal counsel, designated authority contact.
IEC 62443-3-3:2019 FR 5 Restricted data flow + FR 1 SR 1.1	Hardware-enforced zone boundary (Bifrost Unit at L3), scoped tunnel access.	Security level assignment per zone, documented conduit policies, periodic penetration testing.
BEK 260 §62: mandatory network segmentation during vendor access	Bifrost Unit in DMZ, masquerading, outbound-only OT posture.	Network architecture documentation, vendor VLAN policies, segmentation verification testing.
BEK 260 §74: alternative communication for incident response	Bifrost Unit over 4G/LTE provides out-of-band access independent of primary WAN.	Tested fallback communication procedures, documented alternative access paths.
CER Directive: supply chain supervision	Cross-vendor session audit trail, per-engagement isolation via SessionGuard VMs.	Cross-sector resilience assessment, supplier qualification program, periodic supply chain review.

IMPLEMENTATION REQUIREMENTS FOR SCENARIO 4

Scenario 4 brings the most controls together. The following deployment decisions make each layer carry its weight:

- **OT-IDS placement:** position OT-IDS visibility downstream of the Bifrost Unit (on the decrypted L1/L2 traffic). DPI on Modbus / OPC UA / S7comm needs the cleartext, so the architecture must give the IDS a tap point past tunnel termination.

- **Pair recording layers:** SessionGuard is designed to capture the operator side; OT-IDS packet captures cover the wire side. Together they answer 'who did what' and 'what hit the protocol' - both questions an incident review needs.

- **Data diode role:** a certified data diode provides unidirectional transfer for log export and Historian replication. Deploy it where one-way movement is mandated; treat it as a transport guarantee, not a replacement for monitoring.

- **Time-bound Direct Tunnel Access:** operate Bifrost Manager on the Advanced plan or Dedicated Cloud tier, which enables Time-Based Access for Direct IP Tunnel so subnet mappings can be made time-bound. This converts the default-permanent posture to default-just-in-time, matching NIS2 Art. 21(2)(i) intent.

MATURITY PROFILE:
MINIMUM VIABLE VS TARGET STATE (SCENARIO 4)

Scenario 4 is the most layered scenario. Minimum viable already brings most of the control set in place; target state hardens the trust boundaries and adds full diode-protected one-way transport for the most regulated environments.

Capability	Minimum viable (Scenario 4 floor)	Target state (Scenario 4 ceiling)
Identity	Bifrost Manager with enterprise SSO (Dedicated Cloud / on-premises tier); RBAC and JIT in place.	Hardware-token MFA on admin accounts; impossible-travel detection; policy four-eyes principle on access scope changes.
Recording	SessionGuard per engagement on customer-deployed VMs.	SessionGuard + OT-IDS packet capture, both correlated at SIEM.
Network boundary	Bifrost Unit at L3 / DMZ, outbound-only.	Bifrost Unit + a certified data diode for one-way log export and Historian replication; segmentation verified by periodic pen-test.
File handling	Vendor file uploads logged and reviewed.	Inline file security gateway on every Direct Tunnel Access upload (multi-engine + content disarm/reconstruction).
Multi-customer isolation	Separate SessionGuard VMs per customer engagement.	Separate Bifrost Manager tenants per customer engagement; cross-tenant data flow architecturally segregated at the tenant boundary.

PRODUCT REFERENCE

Cross-reference: Part 1, Comparative summary and Integration compatibility matrix.

FIGURE 6. BifrostConnect product stack

Three layers: hardware foundation, access methods, and governance and recording.

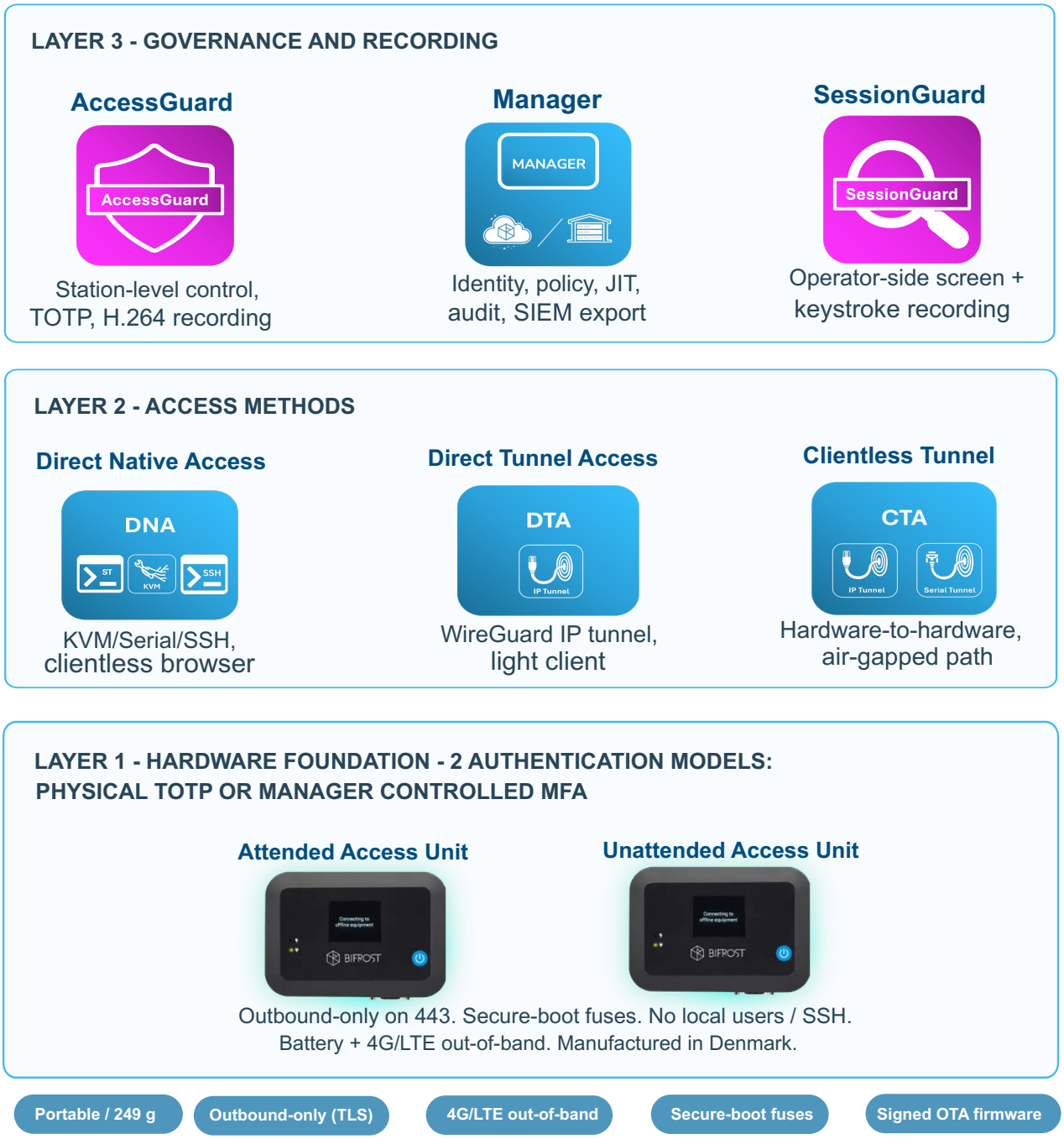
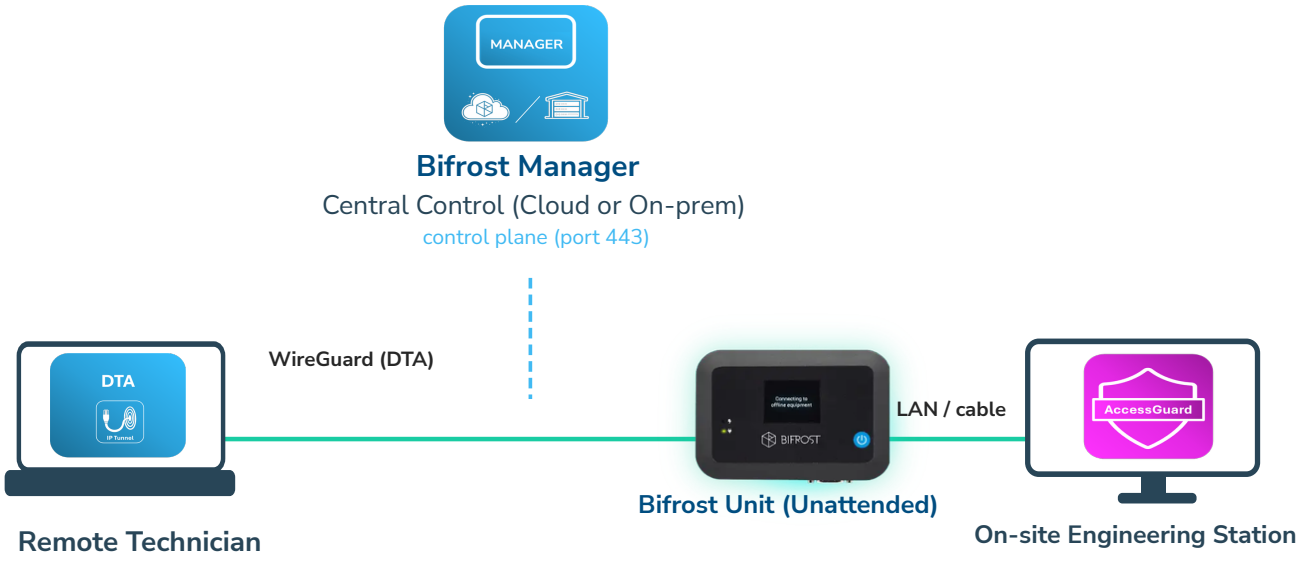


Figure 6. BifrostConnect product stack. Three layers: hardware (Bifrost Unit), access methods (DTA, DNA, CTA), and governance and recording (Bifrost Manager, AccessGuard, SessionGuard).

FIGURE 7. Direct Tunnel Access with AccessGuard

The canonical Scenario 1 and 2 pairing: AccessGuard on the station, Bifrost Unit outbound-only.



Direct Tunnel Access (DTA)

WireGuard IP tunnel via a light installed client, connecting to a Bifrost Unit in the OT environment. Subnet mappings enable scoped access to multiple endpoints for the session duration only.

The Bifrost Unit initiates the connection outbound on port 443: OT calls out, OT never accepts inbound.

AccessGuard (AG)

Station-level access governance on the on-site Windows engineering station: local MFA (TOTP), scoped application launch, and endpoint-side H.264 session recording (DPAPI-encrypted, stored on the OT network).

Bound to localhost (127.0.0.1:7531). No network exposure of the agent.

Figure 7. Direct Tunnel Access with AccessGuard, the canonical Scenario 1 and 2 pairing. Vendor uses the station's installed software while AccessGuard is designed to enforce local control on the OT station and the Bifrost Unit provides outbound-only WireGuard tunnelling.

FIGURE 8. Direct Tunnel Access with SessionGuard

The canonical Scenario 3 and 4 pairing: SessionGuard records the vendor session to a customer VM.

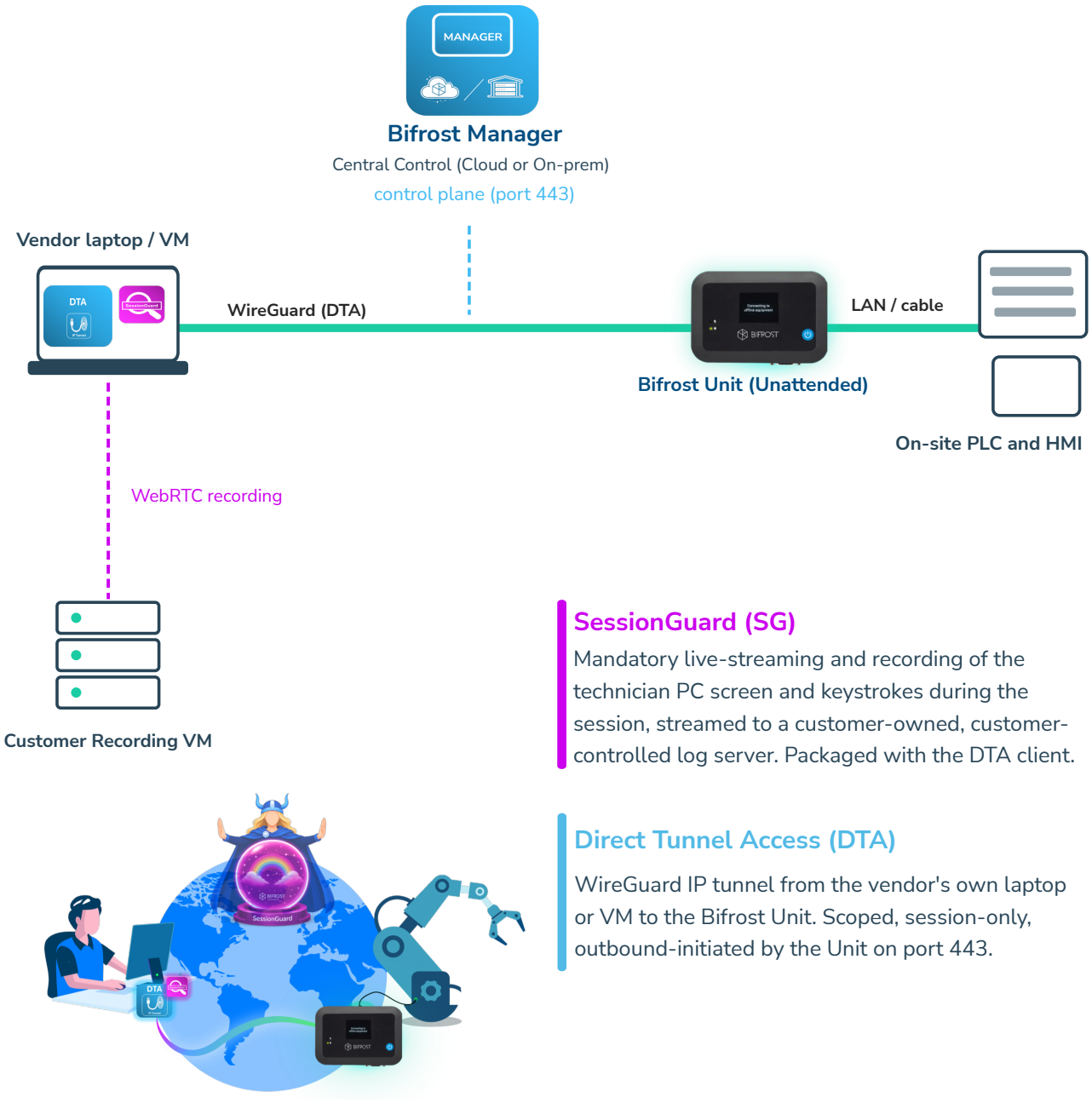


Figure 8. Direct Tunnel Access with SessionGuard, the canonical Scenario 3 and 4 pairing. Vendor brings own laptop or VM; SessionGuard inside DTA is designed to capture session video and keystrokes at the vendor application and stream them outbound to a customer recording VM.

COMPATIBILITY MATRIX

Product	Access type	Role	Primary scenarios
Bifrost Unit	Hardware gateway	Physical access broker. 124 mm × 87 mm × 27 mm, 249 g, battery (~1 hour without charge), 6 GB internal storage, WiFi + LTE built-in, Ethernet, Serial, HDMI, USB-C, SIM card slot. Outbound-only on port 443. Manufactured in Denmark. Industrial embedded Linux; signed, OTA-only firmware; non-reversible secure-boot fuses.	All scenarios
Direct Tunnel Access (DTA)	IP tunnel (with client)	WireGuard-based identity-bound IP tunnel. Scoped subnet mappings. Operator PC gets temporary, scoped network connectivity.	2, 3, 4
Direct Native Access (DNA)	KVM / Serial / SSH (clientless browser)	WebRTC video stream. No network-layer connectivity. Operator PC never joins OT network. Highest isolation.	1, 3 (commissioning, incident response)
Clientless Tunnel Access (CTA)	IP / Serial tunnel (no client software, hardware-to-hardware)	Pure hardware-to-hardware encrypted tunnel. Requires a Bifrost Unit on both the operator and the OT environment side. No software on either side; only active while the session is live.	2, 4
AccessGuard (AG)	Application-level access control	Station-level access governance on the on-site Windows engineering station. Compatible with Direct Tunnel Access and Clientless Tunnel Access; not applicable to Direct Native Access. Localhost agent. Mandatory TOTP. H.264 session recording. DPAPI encryption.	1, 2

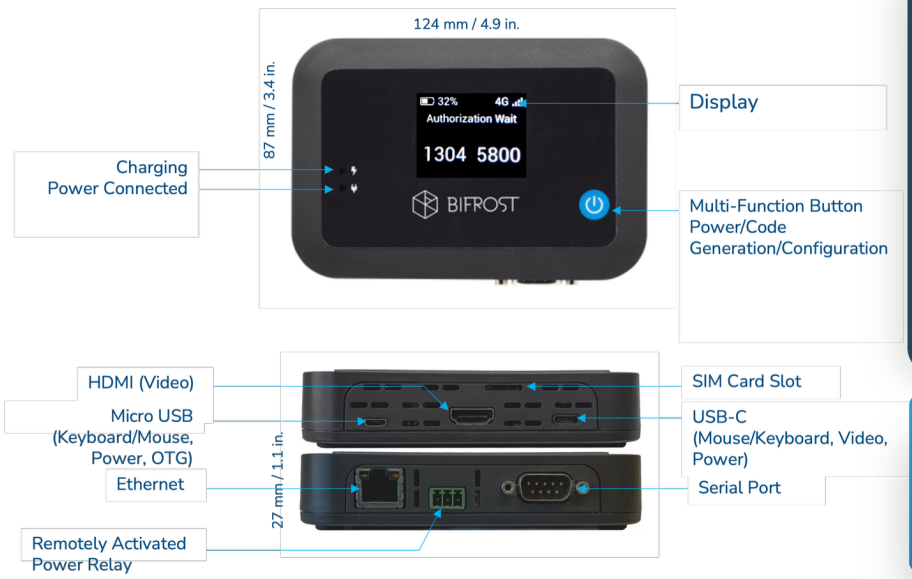
Product	Access type	Role	Primary scenarios
SessionGuard (SG)	Operator-side recording	WebRTC screen + keystroke recording on the technician PC. Designed to operate with Direct Native Access and Direct Tunnel Access. The recording engine is designed to be packaged with the Direct Tunnel Access client, so the client would be installed on the technician PC even when another access type carries the session. Customer deploys the recording log server.	3, 4
Bifrost Manager	Governance platform	Identity, groups, policy, JIT, audit log, SIEM integration. SSO available on Dedicated Cloud / on-premises.	All scenarios
Direct File Transfer	File transfer (online)	Identity-bound file transfer over the Bifrost Unit's outbound channel. Audited.	All scenarios
Offline File Transfer	File transfer (air-gapped)	Air-gapped media transfer pattern. Used in Scenario 3/4 where the OT zone has no IP path.	Air-gapped operations

HARDWARE SPECIFICATIONS:

ATTENDED VS UNATTENDED BIFROST UNITS

Each Bifrost Unit is produced as either Attended or Unattended, embedded in firmware for the product lifespan.

- Attended Units display an 8-digit TOTP on-screen that the operator must enter, and include a physical disconnect button for on-site authorization.
- Unattended Units allow admin-initiated sessions without on-site presence, through the Bifrost Manager. The two are not interchangeable at runtime.



BifrostConnect offers **two authentication models** depending on security and access requirements:

1. Attended Access: 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.
2. Unattended Access: Enables **seamless remote access** through **BifrostConnect 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.

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 build in.

WHY THIS ARCHITECTURE DIFFERS

Cross-reference: Part 1, Implementation approaches.

Part 1 notes that a best-practice OT remote access architecture must close the path when no session is active, bind every action to a named individual, and keep the trust boundary out of the enterprise attack surface.

This section shows how BifrostConnect differs architecturally from the three most common alternatives in the context of OT access. The comparison applies to trust boundary placement in OT environments specifically. Modern Zero Trust and SASE architectures address related problems in IT environments through different patterns; the discussion below is deliberately scoped to OT.

THREE QUESTIONS THAT EXPOSE THE DIFFERENCE (IN OT CONTEXT)

- Where is the trust boundary? In a VPN it is the network edge; in ZTNA it is a cloud broker; in a jump host it is a reachable server; in BifrostConnect it is a physical hardware device the operator never logs into. In OT, a trust boundary that requires inbound connectivity is a trust boundary that can be probed, scanned, or exploited from the vendor or internet side.

- What is the attack surface when no session is active? A VPN concentrator on the OT boundary is always on. A jump host in the DMZ is always listening. BifrostConnect's Bifrost Unit maintains only an outbound connection and listens on no inbound port. This is the OT Island principle in practice: OT calls out, OT never receives.

- What is the failure mode if the broker is compromised? A compromised VPN concentrator exposes the OT network. A compromised jump host gives an attacker a dwell position inside L3. A compromised Bifrost Unit cannot be reached inbound, cannot be logged into locally, and cannot boot alternative firmware. The Service-side trust boundary is a separate hardening surface (see Architectural transparency below).

ARCHITECTURALLY, BIFROSTCONNECT IMPLEMENTS THE OT ISLAND PRINCIPLE

OT initiates outbound, OT never accepts inbound. The Bifrost Unit is the enforcement point of that principle at the OT boundary. The consequence is that the OT environment remains an island: reachable only through explicitly activated, time-limited, identity-bound sessions brokered by the Bifrost Unit's outbound connection.

COMPLEMENTARY LAYERS: WHERE TO KEEP YOUR INCUMBENTS

BifrostConnect occupies the access-and-governance layer. Defence in depth keeps each layer with its specialist. The following pairings produce a stronger architecture than any single product attempting to cover the full stack:

- Endpoint Detection and Response on engineering stations: keep your EDR vendor for malware detection on the station. AccessGuard governs who connects and what they do; EDR observes what runs once they are in. The two are complementary recording layers.

- Network intrusion detection on the OT network: keep an OT-IDS for protocol-level DPI. Co-deploy alongside BifrostConnect, with both feeding the SIEM. Correlation produces the joint forensic view that neither product alone can.

- Credential vaulting at enterprise scale: keep your PAM platform for credential rotation and vaulting. BifrostConnect sits upstream as the access-and-audit layer. Mapping ownership cleanly avoids overlap and keeps the credential audit trail in PAM.

- Industrial telemetry backbone: BifrostConnect is the governance-and-access layer for human sessions; keep your industrial telemetry transport (OPC UA aggregator, MQTT broker, historian) for continuous machine-to-machine data flow.

- IT remote access: for enterprise IT with standard endpoints and SaaS applications, ZTNA platforms cover the IT use case. BifrostConnect is the OT-specific complement - keep both, scoped to their respective domains.

CO-DEPLOYMENT CATEGORIES

Cross-reference: Part 1, Implementation approaches.

BifrostConnect is the governance and access layer. Defence in depth requires monitoring, inspection and isolation layers. The relationships below are co-deployments: BifrostConnect and the co-deployed products operate independently on the same network, correlated at the SIEM layer. Unless stated otherwise, there is no API-level integration with shared data model or certified integration tests.

FIGURE 9. Co-deployment with OT security specialists

BifrostConnect handles access and governance; specialists handle detection. Correlation at the SIEM.

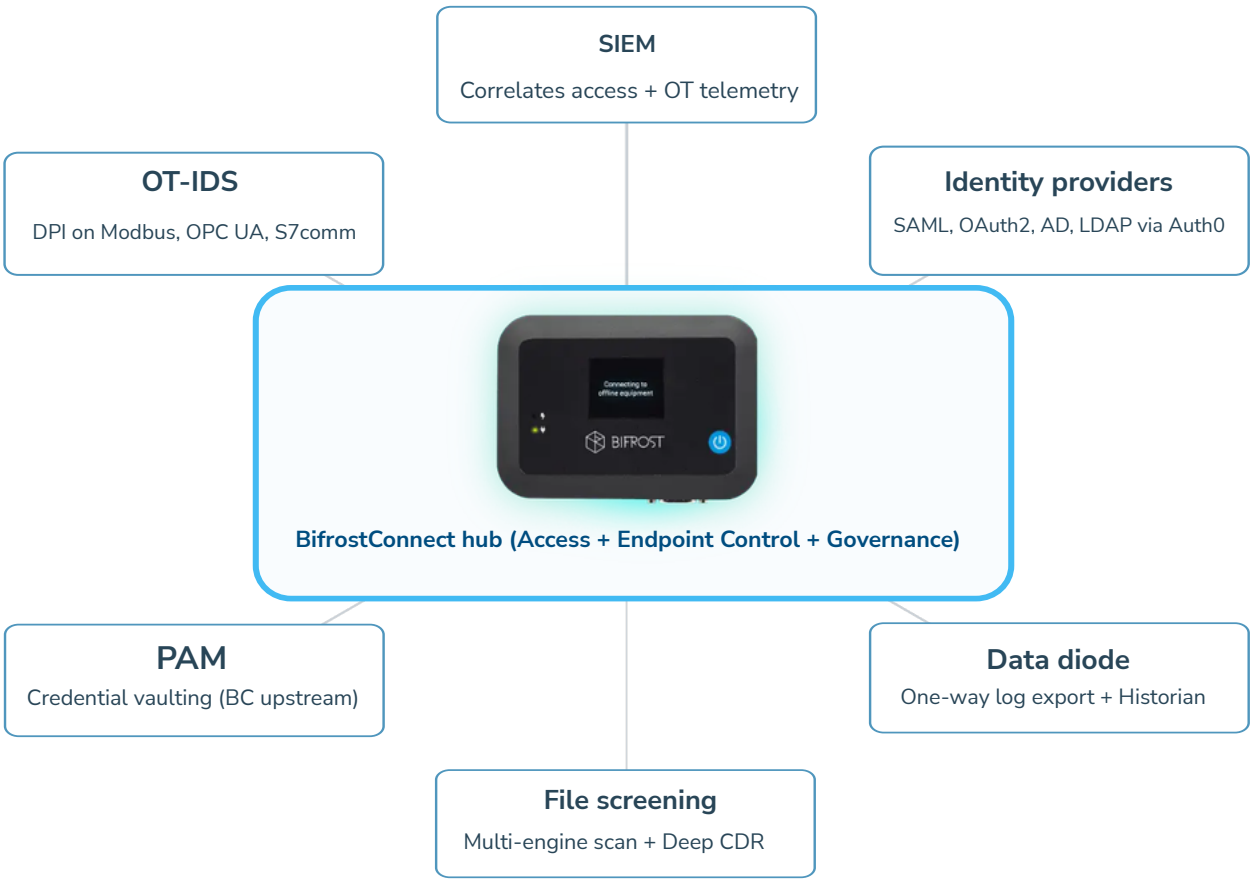


Figure 9. Co-deployment with OT security specialists. BifrostConnect handles access and governance; specialist tools (OT-IDS, EDR or XDR, PAM, NDR) handle detection, monitoring, and response. SIEM correlates session evidence with specialist alerts.

MATRIX - SUGGESTED OPTIONAL CO-IMPLEMENTATIONS

Product category	Role	Co-deployment pattern
OT-IDS platforms	Deep packet inspection on Modbus TCP, OPC UA, S7comm, IEC-104 and equivalent.	Deploy OT-IDS on L1/L2 traffic after Bifrost Unit decryption. Forward alerts to customer SIEM alongside Bifrost Manager events.
SIEM platforms (Splunk, Sentinel, IBM QRadar)	Centralised correlation of access and OT telemetry.	Bifrost Manager native SIEM export (Dedicated Cloud / on-premises). Correlation of BifrostConnect events with OT-IDS alerts at the SIEM.
Identity providers (enterprise IdP / on-prem directory)	Enterprise identity federation.	SAML 2.0, OAuth 2.0, AD, LDAP via Auth0. SSO available on Dedicated Cloud / on-premises.
Certified data diode	Unidirectional log export, file security gateway (malware scanning, 30 AV engines, content disarm/reconstruction), one-way database replication.	Place diode between OT logging infrastructure and enterprise SIEM destination. Inline file security gateway with Direct Tunnel Access for vendor file uploads.
PAM platforms	Enterprise privileged credential vaulting.	BifrostConnect sits upstream of the credential layer. Co-deployment: Manager handles access authentication, PAM handles credential rotation and vaulting.

ARCHITECTURAL TRANSPARENCY: HARDENING THE TRUST BOUNDARIES

BifrostConnect introduces two trust boundaries that the customer's deployment decisions can harden directly: the BifrostConnect Service (the outbound endpoint of every Bifrost Unit) and the Bifrost Manager tenant (the access governance plane). This section is written for the deployment architect: each subsection names the boundary, the threat model around it, and the deployment options that strengthen it. Treat it as the hardening checklist, not a list of unmitigated risks.

HARDENING THE SERVICE-SIDE TRUST BOUNDARY

The Bifrost Unit holds an outbound-only posture and listens on no inbound port. The outbound channel to the BifrostConnect Service (gotobifrost.com on port 443) carries session signalling, firmware update verification, and management commands. The deployment options below progressively reduce the blast radius of a Service-side compromise.

Architectural properties already in place

- **Bifrost Units do not accept arbitrary Service commands:** every session initiation requires explicit user authentication and (for Attended Units) physical TOTP entry. The Service can request signalling, not silent take-over.
- Firmware updates require signed images verified on the Unit before application. eFuse-enforced secure boot means an attacker with Service control still cannot install alternative firmware.
- Session content is encrypted end-to-end between operator and Bifrost Unit (DTLS-SRTP for WebRTC, WireGuard for Direct Tunnel). The Service relays signalling and cannot decrypt session content.

Deployment options to harden further

- Choose Dedicated Cloud or on-premises Manager: this confines the signalling channel to a single customer's infrastructure, sharply reducing blast radius compared to shared-tenant.

- Federate the Service authentication layer to your enterprise IdP and apply your strongest MFA policy (hardware tokens, conditional access). The signalling channel becomes only as exposed as your IdP.
- Set short TOTP lifespans on Attended Units (default 60s, configurable) so a stolen credential plus a stolen TOTP loses validity quickly.
- Forward Service-side authentication events to your SIEM and alert on anomalies (impossible-travel logins, MFA bypass attempts, unusual session-initiation patterns).
- For the highest-assurance environments, document which assets sit behind which Bifrost Unit so an organisational response plan can scope and isolate quickly if a Service-side anomaly is detected.

HARDENING MANAGER ADMIN GOVERNANCE

The Bifrost Manager is the governance control plane: user provisioning, group membership, access policy, audit log retention, SIEM forwarding. Admin compromise is therefore a high-impact event. The deployment options below make admin compromise harder and detection faster.

Architectural properties already in place

- Mandatory MFA on Manager admin accounts (Auth0). MFA is not optional and cannot be disabled at the org level.
- Audit logging captures every admin action (group changes, policy edits, user provisioning). Forwarded to customer SIEM on Dedicated Cloud / on-premises tiers.
- Least-Privilege role model: Privileged User scope is bound to assigned groups; Admin scope is bound to the organisation. Scope creep requires an explicit role change.

Deployment options to harden further

- Federate admin sign-in to your enterprise IdP, then apply hardware-token MFA, conditional access, and impossible-travel rules already in place for IT admins.

- On Dedicated Cloud / on-premises, restrict Manager access to specific IP ranges or VPN-only paths. The Manager becomes a corporate-network application rather than an internet-exposed one.

- Forward Manager admin actions to SIEM and tune detection rules: bulk group-membership changes, sudden policy relaxations, off-hours admin sign-ins, role escalations.

- Operate a four-eyes principle on policy changes: require a second admin to approve material changes to access scope. Document the approval in the runbook so it is auditable. For organisations where four-eyes must be product-enforced rather than procedurally enforced, the Bifrost Manager policy engine is designed to support this pattern.

- For multi-customer service providers, deploy separate Manager tenants per customer engagement to prevent cross-tenant data bleeding at the governance layer.

IMPLEMENTATION HARDENING GUIDANCE

Cross-reference: Part 1, Compliance maturity matrix.

Part 1's compliance maturity matrix distinguishes 'required', 'best practice' and 'structurally unsolvable'. This section is the deployment-side companion: each subsection names a deployment decision and the secure-by-default implementation that delivers the compliance evidence Part 1 calls for. The intent is to ship a hardened deployment, not to enumerate gaps.

RECORDING ARCHITECTURE: CHOOSE THE RIGHT TIER PER SCENARIO

Enforced session recording is the evidence backbone of every scenario. Choose the recording layer that matches where the programming software lives:

- **Software on engineering station (Scenarios 1 and 2):** deploy AccessGuard. H.264 video, DPAPI-encrypted at rest on the station.
- **Software on vendor PC (Scenarios 3 and 4):** the recording layer is SessionGuard, designed to capture WebRTC screen and keystrokes into a customer-deployed VM.
- **For protocol-level evidence (Modbus, OPC UA, S7comm, IEC-104):** co-deploy an OT-IDS that captures the wire side. The two recording layers together give the complete forensic chain.

The 'forced session recording, no matter where your programming licenses are located' claim holds when the appropriate layer is deployed. The deployment step is what makes the claim real; treat it as part of go-live, not as an optional feature.

Personal data note. Session recordings produced by SessionGuard or AccessGuard typically contain personal data within the meaning of the EU General Data Protection Regulation (GDPR). The technical enforcement described here does not remove that obligation: the deployment architect must define a retention period, storage location and access control, data-subject rights handling, and a lawful processing ground for the recordings, independently of NIS2 status. See Part 1, 'Personal data note', for the principle-level statement.

SESSIONGUARD DEPLOYMENT:
CUSTOMER RESPONSIBILITIES FOR EVIDENCE INTEGRITY

SessionGuard is designed to run on a customer-deployed and customer-maintained VM, one per vendor engagement. Plan the VM as a first-class deployment artefact, not an afterthought:

- **Build, ownership and patch responsibility** assigned before the first session - typically OT operations or central IT.
- **Customer-controlled storage for recordings** so the evidence chain is auditable and never leaves the customer's perimeter.
- **Acceptance test as a go-live gate:** confirm (a) sessions cannot start when the VM is unreachable, (b) recordings land in customer storage, (c) tampering alerts reach the SOC. Document the test result in the runbook.
- **Per-engagement isolation:** separate VMs for separate customer-vendor relationships so cross-tenant evidence cannot bleed.

ACCESSGUARD DEPLOYMENT:
SCOPE AND SUPPORTED CHANNELS

AccessGuard operates as a localhost-only agent on the engineering station, bound to 127.0.0.1:7531. The vendor accesses it from the engineering station itself; the agent is not exposed on the OT network, which prevents lateral movement. The supported delivery path is the AccessGuard browser session itself; KVM switches, TeamViewer and AnyDesk are out of scope.

Make AccessGuard the only authorized vendor delivery path on the station, and remove or block the others as part of the access policy. The recorded path becomes the only path - which is the evidence model the auditor expects. AccessGuard's feature set and hardening continue to mature; track product release notes alongside scheduled operations changes.

DIRECT TUNNEL ACCESS:

- **Direct Tunnel Access client (macOS and Windows, installed lightweight client):** supports multi-user parallel access and subnet mapping. Does not currently support port-forwarding. Use when the vendor's workflow benefits from one-to-many or many-to-one access patterns through the Bifrost Manager, and the technician PC can have the lightweight client installed.

TIME-BASED ACCESS:
ENABLE THE ADVANCED ACCESS MANAGEMENT MODULE

Out of the box on the Plug & Play plan, Direct Tunnel Access subnet mappings are permanent. Organisations operating under NIS2 Art. 21(2)(i) or BEK 260 §55 stk. 2 should operate Bifrost Manager on the Advanced plan or Dedicated Cloud tier, which enables Time-Based Access for Direct IP Tunnel so subnet mappings inherit a default time bound. This converts the default-permanent posture to default-just-in-time, which matches the Zero Standing Privilege framing in Part 1.

DIRECT NATIVE ACCESS:

CHOOSING IT FOR THE RIGHT WORKLOAD

Direct Native Access streams video via WebRTC. It carries the highest isolation (no IP path) and is the right default for screen-level commissioning, incident response, and legacy gear interaction. For high-latency WAN paths or slow LTE links, prefer Direct Tunnel or schedule the work over a higher-bandwidth path. Match the access model to the task; do not retrofit by exception.

AIR-GAPPED PATH:

WHEN TO DEPLOY A BIFROST-TO-BIFROST TUNNEL

A Bifrost-to-Bifrost tunnel (Clientless Tunnel Access) requires a Bifrost Unit on both the operator and the OT environment side. The hardware footprint doubles, but so does the control plane: the tunnel terminates on dedicated hardware on each end, with no general-purpose laptop in the path. Deploy this pattern when the assurance level demands it - typically BEK 260 §62 segmentation requirements during vendor access on Class 1 or 2 sites.

SIEM AND SSO:

DEPLOYMENT TIER REQUIREMENTS

Native SIEM forwarding and enterprise SSO (SAML 2.0, OAuth 2.0, AD, LDAP via Auth0) are delivered on BifrostConnect Dedicated Cloud and on-premises Manager tiers. Procure the right tier at the start so the SSO trust chain and SIEM correlation pipeline are established before the first vendor session - retrofitting after go-live is a documentation burden the rollout can avoid.

MULTI-CUSTOMER ISOLATION:

DELIBERATE SEGMENTATION

Service providers and vendor technicians servicing multiple customers should isolate each engagement deliberately:

- **Separate SessionGuard VMs per customer engagement**. Recordings never share storage between customer relationships.
- **Separate Bifrost Manager tenants for separate customer contracts;** or, where a single tenant is preferred, scoped groups with explicit tenant-level access boundaries.
- **Document the isolation model in the engagement contract** so the customer auditor can trace the segmentation evidence.

FIRMWARE INTEGRITY:

COMPENSATING CONTROLS DURING REMOTE UPDATE

Remote firmware updates are moments of heightened risk on OT assets. The Bifrost Unit's own firmware updates are signed, postponed during active sessions, and verified before application. For OT endpoint firmware updates conducted through the Unit, layer compensating controls so the update path matches the evidence requirements:

- Stage the firmware on a customer-controlled file server before the session, not on the vendor's laptop.
- Validate hash and signature against the vendor's published baseline before the update is applied.

- Test rollback in a non-production environment first; confirm the rollback path works.
- Record the entire update session in SessionGuard or AccessGuard so the change is reconstructable.

WHAT BIFROSTCONNECT DOES NOT PROTECT AGAINST

Part 1 closes with a residual-risk section listing what no architecture can solve on its own. This section is the deployment-side companion: a deliberate enumeration of what BifrostConnect does not protect against, written so the procurement reviewer, the auditor, and the security architect see the same boundary the engineering team does. The intent is operational honesty, not understatement of capability.

Compromise of the vendor endpoint before the session opens. If a vendor laptop is already compromised with a keylogger, a remote-access trojan, or in-process malware, the BifrostConnect session faithfully transports whatever the operator does on that laptop. SessionGuard is designed to capture the evidence; AccessGuard is designed to scope the application surface; neither prevents legitimate-looking malicious instructions from reaching the OT endpoint during an authorised session. Mitigation lies in vendor endpoint hygiene contracts, EDR on the technician PC, and (where the workload allows) preferring Direct Native Access (KVM) over Direct Tunnel Access so the vendor PC does not gain IP-layer access at all.

Compromise of the identity provider or MFA layer. BifrostConnect relies on Auth0 for Manager-side MFA and on the customer's federated identity provider for SSO on Dedicated Cloud and on-premises tiers. A compromise of Auth0 or of the customer IdP undermines the identity binding of every session that depends on it. The Hardening Manager Admin Governance section names the deployment options that reduce the blast radius (federation, hardware-token MFA, IP allowlisting, four-eyes principle on policy changes); the residual exposure is the assurance level of the upstream identity infrastructure itself.

Misuse during a legitimately approved session. An authorised technician within an approved session retains authority for the duration of that session. Session recording (where deployed) and SIEM-forwarded alerts on anomalous command sequences support detection and revocation; they do not prevent the action while it occurs. This is the classic insider-threat residual that Part 1 addresses through the procedural controls (background checks, two-person rules for high-risk work, separation of approval authority).

Threat vectors outside the third-party access scope. Phishing of asset-owner staff, IT-side compromise that pivots into OT through other paths, SOHO-router compromise of the kind Volt Typhoon uses, supply-chain attacks on the OT software the vendor ships, physical-access attacks on the Bifrost Unit hardware, and protocol-level vulnerabilities in the OT endpoint itself are all outside what a remote-access broker can address. BifrostConnect occupies the access-and-governance layer; complete OT defence requires the layered architecture Part 1 describes, with EDR on stations, OT-IDS on the wire, NDR for east-west monitoring, and the procedural and contractual controls Part 1's residual-risk section enumerates.

Naming these limits is itself part of the control envelope. A buyer who knows where BifrostConnect ends can build the rest of the programme without misplaced confidence; a buyer who does not, will discover the limits during an incident.

SECURITY ARCHITECTURE SUMMARY

Based on BifrostConnect Security Documentation, Version 2.2.2 (2026).

FIGURE 10. BifrostConnect product architecture

Management plane, the four access methods, and the twelve security properties of the system.

Direct Native Access	SESSION GOVERNANCE AD-ON: SessionGuard
Direct Tunnel Access	SESSION GOVERNANCE AD-ON: SessionGuard + AccessGuard
Clientless Tunnel Access	SESSION GOVERNANCE AD-ON: AccessGuard

FIGURE 10. BifrostConnect product architecture

Management plane, the four access methods, and the twelve security properties of the system.

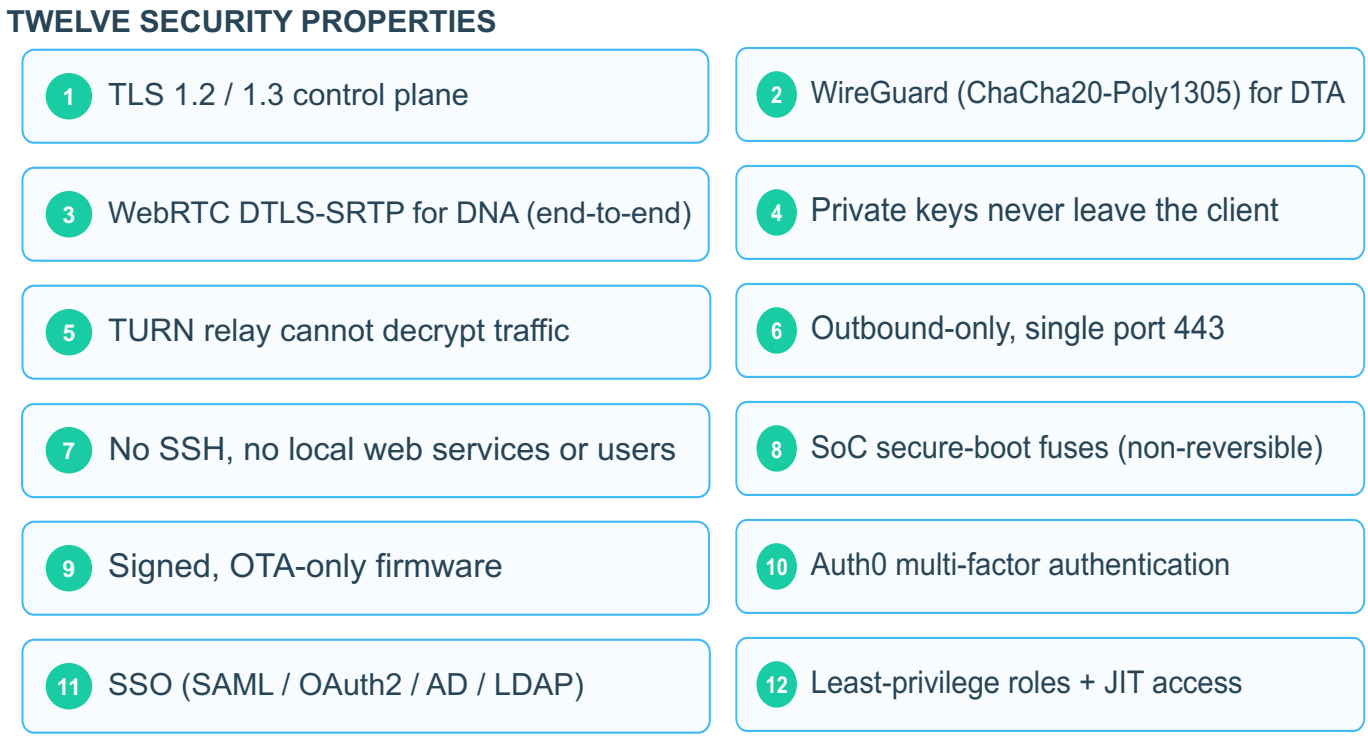


Figure 10. BifrostConnect product architecture. Management layer in the cloud control plane, client-side access types, on-site components, and the twelve security properties that combine to deliver the system.

TRANSPORT AND ENCRYPTION

- Control plane: TLS 1.2 or 1.3 for all HTTPS endpoints and MQTT over WebSocket Secure.
- WireGuard for Direct Tunnel Access traffic, based on Netbird, using ChaCha20-Poly1305 AEAD with Curve25519 ECDH and BLAKE2s (the WireGuard cipher suite).[3]
- WebRTC with DTLS-SRTP for session-based access (Direct Native Access). End-to-end encrypted between browser and Bifrost Unit.

[3] WireGuard cipher suite per the WireGuard whitepaper at https://www.wireguard.com/papers/wireguard.pdf. Retrieved 2026-05-07.

- Private WireGuard keys never leave the client machine.
- Relay service operates as a TURN server and cannot decrypt traffic it relays.

HARDWARE SECURITY OF THE BIFROST UNIT

- Industrial embedded Linux, stripped of non-essential services. Only listening port is 443.
- No physical service ports or debugging interfaces. No local users on the Linux platform.
- Secure-boot enforcement: all fuses on the Bifrost Unit's SoC are burnt at manufacture (non-reversible), preventing boot from alternative storage. The fuse mechanism is a property of the SoC itself; it is distinct from a discrete TPM chip. There are no SSH or local web services, no local users on the embedded Linux platform, and unique device keys are generated and stored on each Unit.
- Direct IP / serial / SSH to the Bifrost Unit is not possible.
- Firmware updates only via BifrostConnect Service using signed firmware. Postponed during active sessions.

IDENTITY, MFA AND ACCESS MANAGEMENT

- Auth0 multi-factor authentication for the Bifrost Manager.
- SSO via SAML, OAuth2, AD, LDAP (Dedicated Cloud / on-premises).
- Least Privilege role model: Privileged User operates within assigned groups; Admin operates within organisation.
- Just-in-Time: session-based access types terminate at session end; Direct Tunnel Access subnet mappings can be time-based or permanent.
- Audit logging for tracking, recording and reviewing actions across the client organisation.

ATTENDED VS UNATTENDED AUTHENTICATION

- **Attended Units:** TOTP generated by physical button press, 60-second default lifespan (configurable by admin). Operator must log in to the Manager or browser session with credentials plus 8-digit TOTP.
- **Unattended Units:** admin-initiated access via Manager with credentials + MFA. TOTP not applicable.
- **Each Unit is either Attended or Unattended;** selection is embedded for the product lifespan.

TELEMETRY AND PRIVACY

- Session duration, count, WAN IP of Bifrost Unit, approximate location (cell tower-based for 4G), battery and signal strength, traffic statistics, unique serial.
- No session content is stored. No GPS on the Bifrost Unit.
- Data stored within BifrostConnect infrastructure. No telemetry shared with Netbird. WiFi passwords hashed on the Unit, not stored in the Service.

BIFROSTCONNECT FOR LEGACY OT EQUIPMENT

Part 1 introduces a section on compensating controls for legacy equipment. This section describes what BifrostConnect can and cannot do for legacy OT and where the boundary lies between BifrostConnect's coverage and the asset owner's supplementary controls.

LEGACY SERIAL CONNECTIONS VIA THE BIFROST UNIT

Bifrost Unit (with serial console port), Clientless Tunnel Access

Many legacy PLCs and RTUs accept only RS-232 or RS-485 serial connections. The Bifrost Unit provides a serial console port and can broker session-based access to a serial device behind it.

The IP-side properties of the brokered session (authenticated operator, time-bounded access, session recording where SessionGuard or AccessGuard is deployed, audit log export to customer SIEM) apply to the IP path between the operator and the Bifrost Unit; the serial side is a controlled extension of that session. The operator never gets a flat IP path to the legacy device.

This satisfies the Part 1 'Serial connections via protocol converters' compensating control.

AIR-GAPPED SYSTEMS: WHERE TO DEPLOY BIFROSTCONNECT AROUND THE GAP

Where the asset owner has a deliberate air gap, the air gap itself is the primary control - and BifrostConnect is not designed to bridge it. The Bifrost Unit needs an outbound IP connection to the BifrostConnect Service to function, so it must sit on the IT side of the gap, never inside the air-gapped OT zone. The strongest deployment pattern uses BifrostConnect to harden the boundary on either side of the gap rather than to cross it:

- **On the IT side:** deploy a Bifrost Unit on the staging workstation that prepares signed media for transfer. Vendor access to this workstation is then identity-bound, time-bounded, and recorded.
- **On the OT side**: keep human-and-procedural brokering in place (controlled media transfer, chain-of-custody, multi-engine malware scanning via a data-diode file security gateway).
- **Combined effect:** BifrostConnect supplements rather than substitutes for the air gap procedures, and the audit trail covers everything the vendor touched on the IT side.

Procure BifrostConnect with this scope in mind: it strengthens the perimeter of an air-gapped installation, but it does not replace the gap.

PROPRIETARY SYSTEMS THAT CANNOT HOST AN AGENT

Bifrost Unit at the boundary, Direct Native Access for screen-level interaction

Many legacy automation platforms cannot run AccessGuard or any other endpoint-resident agent. The applicable BifrostConnect pattern is to wrap the legacy device behind a Bifrost Unit deployed at the boundary of a small dedicated VLAN.

The legacy device contributes nothing to its own security; the Bifrost Unit contributes the identity, time-bounding, recording, and log-export properties externally.

Direct Native Access (KVM, serial, SSH session types) is the typical access modality because the operator interacts with the legacy device through whatever console the device offers, with no modification to the device itself.

The asset owner is responsible for the firewall rules that deny all paths into the dedicated VLAN except via the Bifrost Unit.

OPERATIONAL COMPENSATING CONTROLS FOR LEGACY OT

Some legacy OT failure modes are operational rather than technical: a device with a single shared password, a legacy operating system that cannot be patched, proprietary firmware that the device vendor will not document. BifrostConnect handles the human-session governance around these devices; the asset owner's operational compensating controls handle the rest. The combination is what produces a defensible control envelope:

- **Controlled engagement scheduling:** every vendor touch on a legacy device happens through a Bifrost Unit session, time-bounded, identity-bound, and recorded. The session record is the audit artefact even when the device itself produces none.

- **Supervisor co-presence:** for the highest-risk legacy interactions, require an on-site operator to be present (Attended Bifrost Unit with physical TOTP, or Direct Native Access with operator screen-share). The four-eyes principle compensates for the device's inability to enforce identity itself.

- **Pre- and post-engagement integrity baselines:** capture a known-good baseline before the session (configuration export, firmware hash where readable, file-system snapshot), and re-validate against that baseline after the session. Anomalies surface in the SOC without relying on the device's own logging.

- **Authorized application scope:** where AccessGuard is in scope, scope the launchable applications to exactly what the engagement needs. Where AccessGuard is not in scope, encode the equivalent constraint in the change-management ticket and verify against the recording.

These controls do not change the legacy device. They put the device inside an envelope that is identity-bound, time-bounded, recorded, and reviewable - which is what the regulator is looking for.

FIGURE 11. Incident response lifecycle

BifrostConnect across the five phases; the out-of-band path stays available throughout.

1. Prepare

BifrostConnect: core role

Zero standing privilege, brokered access and recording in place before any incident: the control baseline.

2. Detect

Customer-side (BC supports)

Customer-side activity (SIEM, NDR). BifrostConnect contributes session audit logs as an input, not the detector.

3. Respond

BifrostConnect: core role

Clean out-of-band access for responders over 4G/LTE, with Manager approval and the Bifrost Unit, independent of the WAN.

Island-Mode / Fallback Mode

- Critical systems continue running in isolation
- Access only through BifrostConnect
- Remote support via 4G/Satellite
- Maintain operations without reopening the network

4. Recover

BifrostConnect: core role

Forensic session recordings plus a controlled rebuild path (Manager + Bifrost Unit + AccessGuard / SessionGuard).

5. Learn

Customer-side (BC supports)

Customer-side review. The audit trail and recordings feed the post-incident analysis and control improvements.

The Result

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

Figure 11. Incident response lifecycle. BifrostConnect across the five NIST CSF phases: prepare, detect, respond, recover, learn. The out-of-band path remains available across all five phases; no inbound exposure is introduced during emergency response.

FIGURE 12. Island mode and business continuity

When the production network is down, the out-of-band path keeps essential operations running.

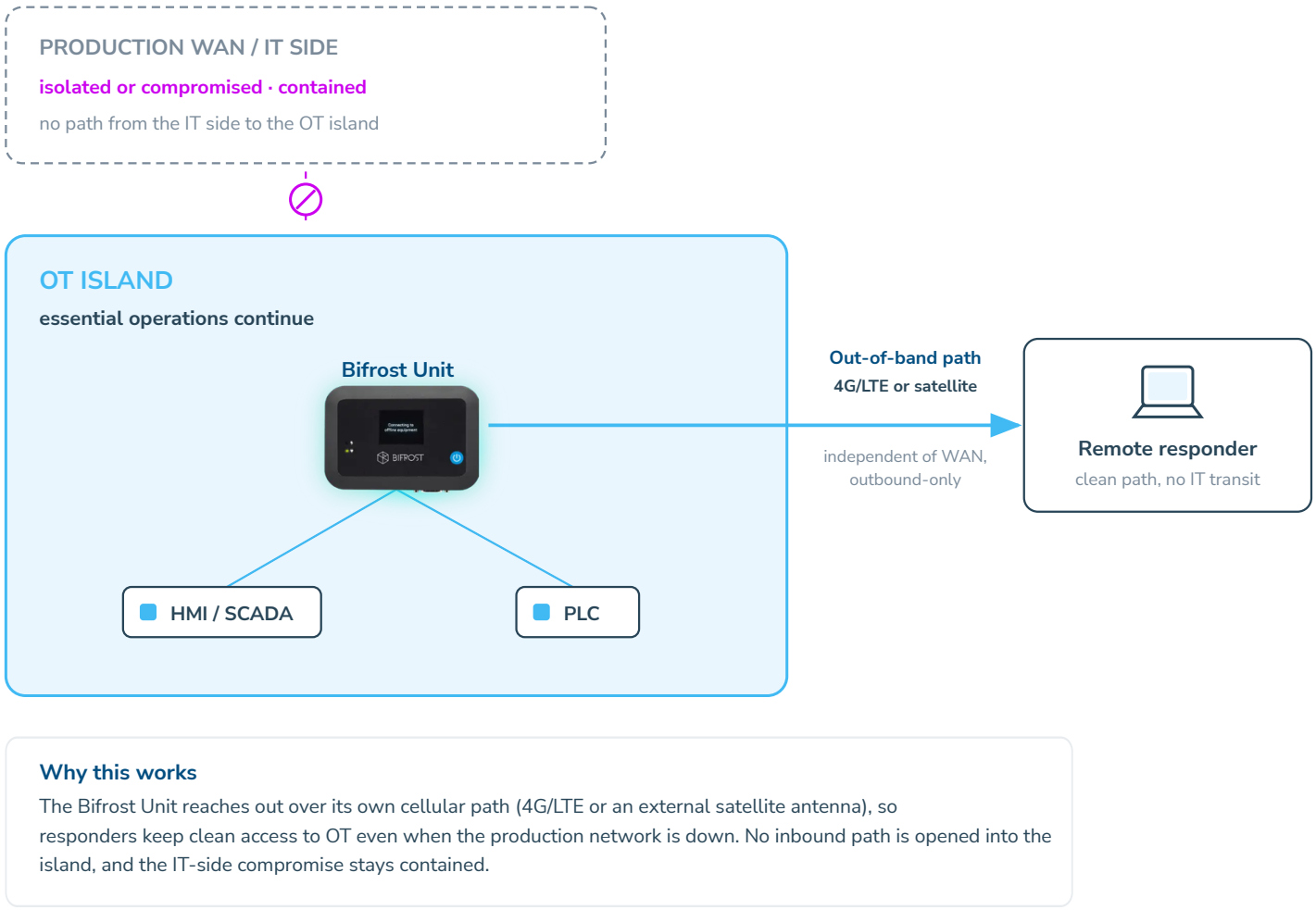


Figure 12. Island mode and business continuity with BifrostConnect. When the production network is isolated or compromised, BifrostConnect's out-of-band LTE path keeps essential operations running while IT-side compromise is contained.

BIFROSTCONNECT IN DEGRADED MODE

Part 1 introduces a section on degraded mode operations: what should happen when the central session broker is unavailable. This section describes BifrostConnect's concrete behaviour in each degraded scenario.

BIFROSTCONNECT SERVICE IS UNREACHABLE (WAN OUTAGE)

Symptom: the Bifrost Unit cannot reach the BifrostConnect Service. New session requests cannot be initiated through the standard path. Existing established sessions are tunnels that have already been negotiated end-to-end and may continue if the tunnel is stable; new sessions cannot start until the WAN is restored.

BifrostConnect behaviour: the Bifrost Unit retries the outbound connection at a configurable interval and resumes normal operation when reachability is restored. The Unit does not accept inbound connections during the outage; the OT Island Principle is preserved.

BIFROST MANAGER IS UNREACHABLE (MANAGER-SIDE OUTAGE)

Symptom: authentication, group lookup, or policy retrieval against Bifrost Manager fails. BifrostConnect behaviour: an active session continues until natural teardown (browser close, TOTP expiry, time-window end); new sessions cannot be authorised while the Manager is unreachable, since identity binding and policy lookup depend on Manager-side services. Audit events are queued locally on the Unit and synchronised to the Manager when reachability is restored. Customers operating under strict NIS2 or BEK 260 obligations should document this dependency in their incident response procedures and confirm that the operational risk profile of a Manager outage matches their organisation's tolerance.

SESSIONGUARD RECORDING TARGET UNREACHABLE

Symptom: the customer-deployed SessionGuard recording VM is offline or unreachable. BifrostConnect behaviour: by default and per documented best practice, sessions should not start when the recording target is unreachable; allowing un-recorded sessions weakens the evidence chain.

For organisations with explicit emergency policies, the Bifrost Unit can be configured to permit a session under temporary local recording with mandatory upload upon recovery; this is a documented break-glass option, not a default. The audit log records the degraded-recording state regardless of which option is chosen.

CONTROLS THAT NEVER BYPASS IN BIFROSTCONNECT

Audit trail. Session audit is captured by the Manager/Service and forwarded to the SIEM; the Bifrost Unit retains no local audit log. Because the Service brokers every session, a session cannot be established while the Service is unreachable, so there is no un-audited degraded session.

Identity. Every session is tied to a named individual by the Manager/Service identity broker; the Bifrost Unit holds no local user store. If the Manager/Service is unreachable, a session cannot be authenticated and is not established (fail-closed).

Approval. A break-glass session requires an admin to have authorised the degraded mode in advance through Manager configuration; the Bifrost Unit does not invent its own approval.

Time-bounding. Degraded sessions expire automatically; degraded mode is not a stable operating state.

The ten sample procurement clauses in Part 1 form the contractual basis for any third-party OT access engagement with BifrostConnect. Specific clause-by-clause coverage is provided to procurement teams on request as part of the engagement onboarding process.

SOURCES AND REFERENCES

SOURCE DOCUMENTS USED IN PART 2

- BifrostConnect, Security Documentation, Version 2.2.2 (February 2026).
- BifrostConnect, AccessGuard product description.
- BifrostConnect, SessionGuard product description.
- Part 1: OT Best Practice Guide, Part 1 (June 2026).

REGULATORY SOURCES (SHARED WITH PART 1)

- Directive (EU) 2022/2555[4], OJ L 333, 14 December 2022.
- Act No. 434 of 6 May 2025 on measures to ensure a high level of cybersecurity (Danish NIS2 Implementation Act).
- Styrelsen for Samfundssikkerhed (SAMSIK), Vejledning til NIS 2-loven, June to August 2025.
- IEC 62443 series: DS/EN IEC 62443-3-3:2019 (system security requirements), DS/EN IEC 62443-2-4:2024 (service provider security programme), DS/EN IEC 62443-2-1:2024 (asset owner cybersecurity programme).
- Executive Order No. 260 of 6 March 2025[5], Danish Ministry of Climate, Energy and Utilities.
- Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren (Danish Executive Order on resilience and preparedness in the energy sector).
- ISO/IEC 27001:2022.
- NIST SP 800-82 Revision 3, Guide to Operational Technology (OT) Security, September 2023.
- NIST SP 800-207, Zero Trust Architecture, August 2020.
- NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.
- Joint NCSC, ASD ACSC, CCCS, CISA, FBI, BSI, NCSC-NL, NCSC-NZ, Secure Connectivity Principles for Operational Technology, 18 March 2024.
- Joint CISA, DoW, DOE, FBI, DOS with NIST contributions, Adapting Zero Trust Principles to Operational Technology[6], 29 April 2026.
- Directive (EU) 2022/2557[7], OJ L 333, 14 December 2022.
- Regulation (EU) 2016/679 (GDPR).

[4] Regulation (EU) 2022/2555 (NIS2 Directive). Retrieved 2026-04-22.
[5] Bekendtgørelse nr. 260 af 6. marts 2025. Retrieved 2026-04-22.
[6] CISA, DoW, DOE, FBI, DOS with NIST contributions, "Adapting Zero Trust Principles to Operational Technology", 29 April 2026. Retrieved 2026-05-04.
[7] Directive (EU) 2022/2557 (Critical Entities Resilience Directive). Retrieved 2026-04-22.

CO-DEPLOYMENT REFERENCES

- OT-IDS platforms: referenced for deep packet inspection on OT protocols. Co-deployment, not API-integrated.
- Data diode category: unidirectional gateway, file security gateway (multi-engine malware scanning, content disarm/reconstruction), one-way log export, one-way Historian/database replication. Referenced for compensating controls.
- Auth0: identity and multi-factor authentication layer used by BifrostConnect Service.
- Netbird: open-source WireGuard-based tunnelling component used by Direct Tunnel Access.

THREAT INTELLIGENCE

- MITRE ATT&CK for ICS. Volt Typhoon: CISA Advisory AA24-038A. Sandworm: Mandiant 'APT44: Unearthing Sandworm' (April 2024).
- SektorCERT, Threat Assessment: The Danish Energy Sector, November 2023.
- CISA ICS-CERT Advisories: Colonial Pipeline (AA21-131A), Oldsmar (AA21-042A, attribution disputed), TRITON (Dragos 'TRISIS malware analysis').
- CISA Advisory AA23-335A (CyberAv3ngers): IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors.

DISCLAIMER

This document is a companion to the Part 1 best-practice framework. Product features described here are accurate as of the publication date (June 2026). Regulatory citations reflect the legal text as of the publication date. Customers should validate enforcement of every stated control during rollout through acceptance testing.

Published by BifrostConnect. Part 2 of a two-part publication. Version 1.21, June 2026. Web: bifrostconnect.com.

Where VPNs end, BifrostConnect.