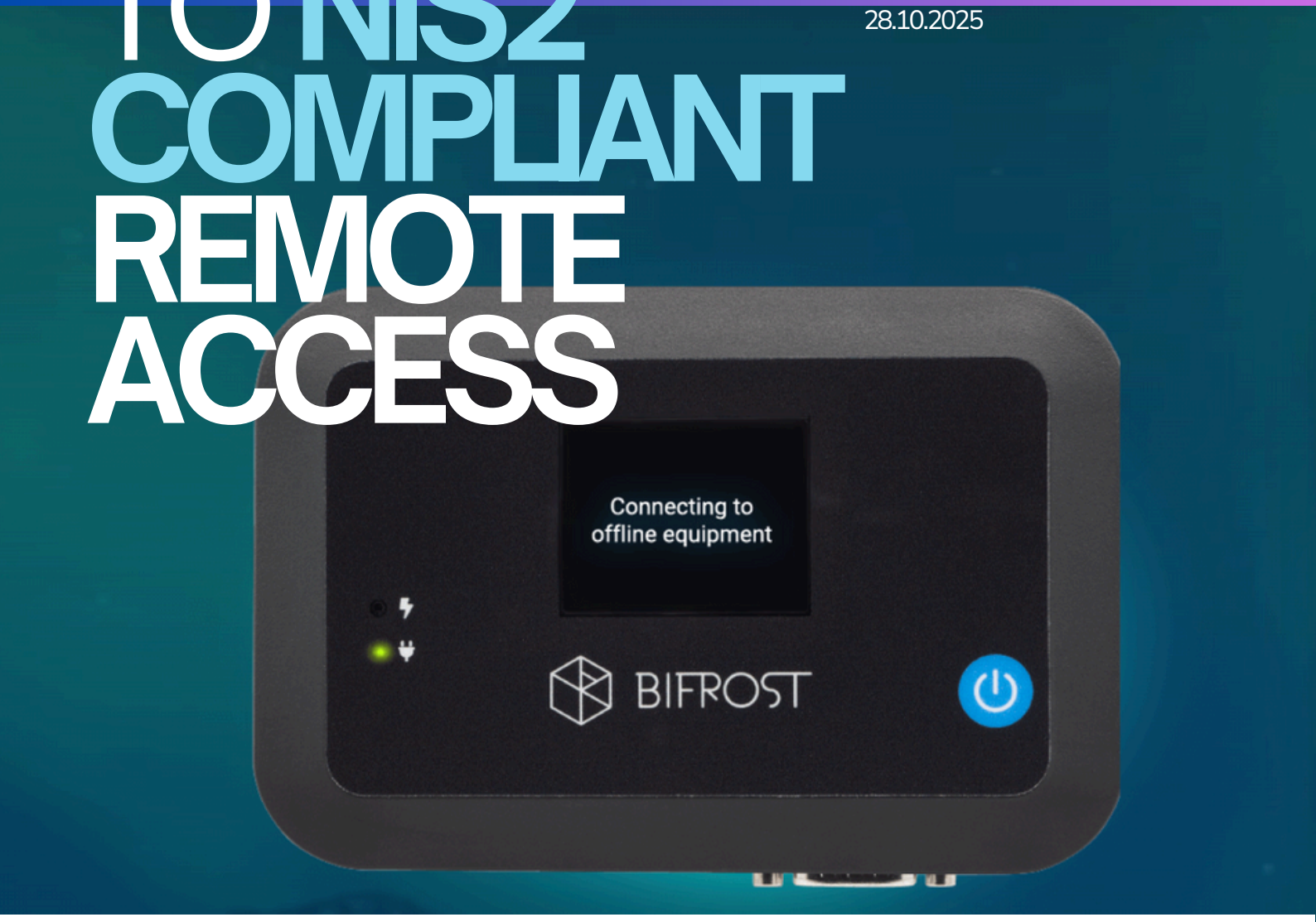
BRIDGE YOUR GAP TO NIS2 COMPLIANT REMOTE ACCESS

MIKAEL VINGAARD. ICSRANGE
& EMILIE FENGER, BIFROSTCONNECT
28.10.2025



Remote access is one of the most overlooked risks under NIS2. This paper explains why, and what to do about it, through actionable strategies and Cybersecurity expert insights.

The NIS2 Directive marks a transformative step in enhancing the cybersecurity resilience across the European Union, especially for organisations who operate within critical infrastructure sectors such as water, energy, transport, health, finance, and digital services. These entities are legally required to implement a range of stringent cybersecurity measures aimed at improving resilience, mitigating risks, and ensuring business continuity.

Introduction:

Remote Access is a NIS2 risk

This white paper is intended for leaders in critical infrastructure who must comply with the NIS2 Directive, especially those responsible for cybersecurity, operational continuity, and third-party/vendor access.

Included in the paper:

- Wy Traditional Remote Access Fails NIS2 Compliance
- Aligning key NIS2 requirements with actionable secure access controls
- Independent insights from cybersecurity expert Mikael Vingaard, ICSRange
- From regulation to reality: How to get real-world compliance through non-persistent, hardware-based remote access

NIS2 introduces legally binding obligations focused on reducing the risk of cybersecurity incidents across critical sectors.

For organisations falling under the "essential" or "important" entity categories, this means implementing controls such as:

- **§ Article 21:** Risk Management & Security Policies
- **§Article 22:** Incident Handling & Business Continuity
- **§ Article 23:** Incident Reporting (within 24 hours)
- **§ Annex I:** Coverage of Energy, Transport, Water, Health, Digital Infrastructure, and more

BIFROST connect

Key Requirements: Why Traditional Remote Access Fails NIS2 Compliance

As cyberattacks grow more sophisticated, especially through remote access points, many legacy remote access methods fall short of modern cybersecurity standards and NIS2 compliance requirements.

Problems with Traditional Remote Access Tools (VPN, RDP, TeamViewer) under NIS2:

- **Persistent Network Exposure:** Always-on VPN tunnels create open pathways that attackers can exploit long after sessions end.
- **No Segmentation Between IT and OT:** Direct access from corporate networks to operational systems breaks required network separation and increases lateral movement risk.
- **Lack of Least-Privilege Control:** Users often receive full administrative rights instead of time-limited, role-based access.
- **Shared or Reused Credentials:** Generic logins eliminate accountability and increase credential theft risk.
- **No Multi-Factor Authentication (MFA):** Legacy RDP and TeamViewer setups often lack enforced MFA, violating NIS2's access-control requirements.
- **No Session Logging or Recording:** Inability to document who accessed what, when, and what actions were taken, - non-compliant with NIS2's auditability clause.
- **Unmonitored Third-Party Access:** No real-time control over when or how vendors connect to critical systems.
- **Static Public IP Exposure:** Endpoints are reachable from the internet, increasing vulnerability to scanning and brute-force attacks.
- **No Out-of-Band Connectivity:** Remote access depends on production networks; if they fail, remote intervention becomes impossible.
- **Lack of Built-in Resilience:** No automatic failover (4G/Wi-Fi/External Satelite), leaving critical infrastructure unreachable during outages.

Key Requirements: Traditional Remote Access VS BifrostConnect

NIS2 Article	Requirement	Where Traditional Solutions Fail	How BifrostConnect Helps
Art. 21(2)(b)	Manage supply-chain and third-party risks	No visibility or control over what vendors do once connected; shared credentials and no assurance that supplier devices are secure.	Each vendor has a unique, time-limited identity and access scope; all sessions are logged and auditable without exposing internal networks.
Art. 21(2)(c)	Maintain resilience under failure conditions	VPN, RDP, and other software tools fail when IT infrastructure or internet connectivity is down.	Mobile, hardware-based unit provides out-of-band connectivity (4G, External Satelite possibility) and continues operation even during incidents.
Art. 21(2)(d)	Ensure secure third-party access	Persistent VPN/RDP tunnels with standing credentials, no expiration, and no accountability.	Time-limited, role-based sessions for external vendors, automatically logged for NIS2 documentation.
Art. 21(2)(e)	Keep systems updated securely	Requires software agents or network access, increasing risk and complexity- often infeasible in OT environments.	Controlled, auditable remote maintenance, patching and configuration updates performed through isolated connections with no internet exposure.
Art. 21(2)(h)	Secure configuration and vulnerability management	Traditional remote tools expose endpoints to the internet and allow unverified configuration changes.	
Art. 21(2)(i)	Define access policies and maintain detailed logs	Shared or static logins; limited or no per-session traceability, often only logged at network level.	Fine-grained, auditable access per user and device; immutable logs stored outside the production network.
Art. 21(2)(j)	Enforce secure authentication and communication	Often lacks MFA and uses unencrypted or partially encrypted sessions.	Physical device-based identity, MFA, and end-to-end encrypted connections with no backdoors.
Art. 22(2)(b)	Enable fast incident response	No access to powered-off or isolated systems; response delayed by network dependency.	Instant BIOS-level access to air-gapped or offline systems, even when powered down.
Art. 22(2)(c)	Ensure documentation and lessons learned after incidents	Traditional tools lack auditable logs for post-incident analysis and compliance reporting.	Automatic activity logs and audit trails that meet NIS2 documentation requirements for incident handling and recovery + option for local session recording of the engineering / SCADA PC.

BIFROST connect

Independent insights from cybersecurity expert Mikael Vingaard, ICSRange

To provide additional expertise, we consulted Mikael Vingaard, an experienced cybersecurity professional and trusted industry advisor. Mikael has worked extensively with critical infrastructure security, IT/OT cybersecurity, and regulatory compliance for over 25 years. His experience includes advising enterprises on cybersecurity strategies, supply chain risk management, and secure remote access solutions.

Disclosure:
Mikael Vingaard has received compensation for his time and expertise in the development of this white paper. His assessments remain independent and based on more than 25 years of experience in IT/OT security.

"

I see three major cybersecurity challenges for industrial companies under NIS2:

1. **Supply Chain Control:**
   Risk assessment and control of remote third-party access to OT is central to NIS2.
2. **Balancing Access & Risk:**
   Organisations must enable secure third-party access without destabilising operations.
3. **Timely Access:**
   Remote access must be secure, auditable, and rapid to meet legal and operational requirements.

Best Practice for companies, to ensure secure third-party access:

- **Avoid shared accounts**: sessions must be traceable to individuals.
- **Use the Principle of Least Privilege:** only grant what's needed.
- **Enforce session logging and active log review.**
- **Define clear SLA clauses outlining vendor security obligations.**
- **Ensure third parties comply with NIS2 and other relevant frameworks.**

Traditional remote access

A traditional remote access like VPN or RDP should often be seen as a door into your home. Whoever has the key can enter and roam freely. Combine that with weak passwords or no MFA, and it's like leaving the key under your doormat.

BifrostConnect:

BifrostConnect allows you to provide ad-hoc secure access where you're in full control.

During a critical incident, for instance, you still need urgent third-party access - but securely.

From regulation to reality:

How to get real-world compliance through non-persistent, hardware-based remote access

Mini-Guide: Secure Remote Access with NIS2:

- Implement non-persistent, zero-trust access – no standing tunnels or permanent credentials
- Enforce MFA and session-based authorisation
- Maintain granular access logs tied to individual users (no shared accounts)
- Ensure end-to-end encryption across all sessions
- Enable emergency access via portable devices
- Support BIOS-level access for offline diagnostics
- Separate remote access from production networks through dedicated out-of-band connectivity

In a world of rising cyber threats, particularly in critical infrastructure sectors, secure remote access is not optional, it's essential. The NIS2 Directive demands a proactive and transparent approach to securing access pathways, especially those used by third-party vendors, service engineers, and IT/OT administrators.

Ready to explore how the solution works?

HOW IT WORKS