WHITE PAPER

NIS 2 Compliance via BlastWave Zero Trust Architectures

BlastWave

TL:DR

The second Network and Information Security Directive, Directive (EU) 2022/2555, moves European cybersecurity from broad guidance to explicit management liability and a defined set of risk-management measures. For essential and important entities, and particularly for the OT-heavy sectors named in its annexes, the obligation is continuous and evidential rather than a one-time checklist.

Two things about NIS2 are widely misstated, and both matter before you plan anything.

NIS2 does not bind you directly.
It is a Directive, not a Regulation. It obliges Member States to legislate. Your actual duties, dates, registration process, reporting route, thresholds, and penalty exposure are determined by national transposing law, which differs by country. There is no single EU-wide compliance deadline for entities, and any vendor who quotes you one is describing something that does not exist.

Article 21(2) sets organizational duties, not product requirements.
The ten measures are policies, procedures, training, governance, and assessment. No product satisfies them. A product supplies technical controls that support them and produces the evidence that they operate. This paper is written on that basis, and where BlastShield does not help it says so.

What BlastShield does provide is a software-defined perimeter that authenticates identity before exposing any network path, conceals protected assets from unauthenticated discovery, segments without physical re-architecture, and records what happened. Those capabilities bear directly on four of the ten measures, support four more, and are out of scope for the rest.

BlastWave

CONTENTS

Whether NIS2 Applies to You, and as What

Essential and important entities carry identical Article 21 obligations.
The difference is supervision, not substance. Essential entities are supervised proactively under Article 32. Important entities are supervised reactively under Article 33, triggered by evidence of non-compliance. Anyone describing important entities as having lighter duties is describing the enforcement posture, not the duty.

Sector and size determine which.
Medium-sized and larger entities in the Annex I and Annex II sectors are generally in scope, with size-independent categories including DNS service providers, TLD name registries, qualified trust service providers, and providers of public electronic communications.

The annex split is worth knowing.
Energy, transport, drinking water, wastewater, and digital infrastructure are listed in Annex I as sectors of high criticality. **Manufacturing sits in Annex II**, other critical sectors. An **Annex I** entity is more likely to be classed as essential and therefore to face proactive supervision. Treating energy, transport, and manufacturing as equivalent in scope terms is a mistake, and it is one the previous version of this paper made.

Managed security service providers are in **Annex I**, under ICT service management. If you are an MSSP serving critical infrastructure, you are in scope at the higher-criticality tier, not merely adjacent to customers who are.

Transposition is Uneven, and That is Your Planning Problem

Article 41(1) required Member States to adopt and publish transposing measures by 17 October 2024. That deadline bound Member States, not entities, and it has not been met uniformly.

As of September 2026, roughly 23 of 27 Member States have national NIS2 law in force. The Commission sent letters of formal notice to 23 Member States in November 2024, issued reasoned opinions in May 2025, and in July 2026 referred Ireland, Spain, France, and the Netherlands to the Court of Justice of the European Union, requesting financial sanctions.

The spread of national dates is wide. Croatia legislated ahead of the deadline. Italy and Lithuania were in force in October 2024. Germany's law took effect on 6 December 2025. The Netherlands followed on 15 August 2026, with no transition period. Austria's principal obligations commence on 1 October 2026. Ireland, France, and Spain have not completed transposition.

What this means in practice.
A multi-country operator faces a patchwork of commencement dates, thresholds, and reporting portals rather than a single program. An entity in a Member State that has not transposed knows the obligations are coming but does not yet have the national text defining them, making it difficult to scope a remediation budget. Neither problem is solved by technology, but both are worth planning around rather than discovering.

Verify your national position before committing to a date. This paper deliberately does not give you one.

Article 20:
The Duty That Falls on Your Board

Article 20 is the provision that changes the conversation inside an organization, and it is frequently omitted from vendor material.

Article 20(1)
Requires management bodies to approve the Article 21 risk-management measures, to oversee their implementation, and provides that they can be held liable for the entity's infringements of that Article.

Article 20(2)
Requires members of management bodies to follow training sufficient to identify risks and assess cybersecurity risk-management practices, and requires Member States to encourage entities to offer similar training to employees.

Article 32(5)
Goes further for essential entities, allowing competent authorities to suspend an authorization and to impose a temporary ban on individuals exercising managerial functions at chief executive or legal representative level.

Approval and oversight are evidenced, not asserted. A management body that has approved a set of measures needs to be able to show what was approved, when it changed, and that it has been operating since. An exportable policy configuration and a change audit trail are the artifacts that make that showing straightforward.

Article 21(2):
The Ten Measures

Coverage on the right uses four words and only these four. Directly addresses means the control satisfies the technical element as written. Supports means it contributes but does not fully satisfy it, and names what else is needed. Provides evidence for means it does not implement the requirement but produces records that demonstrate compliance. Out of scope means BlastShield does not address it.

Because every point is an organizational duty, no row can read "Directly addresses" for the obligation as a whole. What is shown is the technical contribution to it.

Table 1

Measure	What the Directive requires	What BlastShield provides	Coverage
21(2)(a)	Policies on risk analysis and information system security	Asset inventory can be imported from discovery tooling, and the resulting access policy exports as a portable artifact that can be reviewed and version-controlled.	**Supports.** The policy and the risk analysis remain yours to produce.
21(2)(b)	Incident handling	A compromised asset can be isolated by policy change without interrupting unaffected operations. Revoking a user terminates their active sessions within seconds. Remote sessions are recorded to storage for reconstruction.	**Supports containment** and **provides evidence for** investigation. **Out of scope for detection.** BlastShield is a preventive control and performs no anomaly, intrusion, or behavioral detection. Detection comes from a monitoring platform.
21(2)(c)	Business continuity, such as backup management and disaster recovery, and crisis management	Connectivity is established via an encrypted mesh rather than through a single concentrator, removing a common availability chokepoint for remote access.	**Supports**, narrowly. Backup, disaster recovery, and crisis management are **out of scope**.
21(2)(d)	Supply chain security, including security-related aspects of relationships with direct suppliers and service providers	Vendor and contractor access is granted to named systems rather than to a network segment. A connecting contractor cannot discover or reach assets outside their policy. Sessions are recorded. Access is removed within seconds of the account being deleted, and a gateway that was offline applies the revocation upon reconnecting.	**Directly addresses third-party remote access control.** Supply chain security as a whole is considerably broader, covering procurement, supplier assessment, and secure development practices at your suppliers.
21(2)(e)	Security in network and information systems acquisition, development and maintenance, including vulnerability handling **and disclosure**	Equipment that cannot be patched can be made non-responsive to unauthenticated discovery, which reduces the exploitability of a known vulnerability without modifying the device.	**Supports** the maintenance of unpatchable assets. Acquisition, development, vulnerability handling, and disclosure processes are **out of scope**. Note that reducing reachability is not remediation: the vulnerability remains and should remain on your register.
21(2)(f)	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Both failed and permitted access attempts are logged, as are configuration changes. Logs export to a syslog destination you control. The policy configuration exports as a portable artifact.	**Provides evidence for.** The assessment procedure is yours.
21(2)(g)	Basic cyber hygiene practices and cybersecurity training	Removing passwords from the access path removes a recurring class of hygiene failure, including default credentials, reuse, and credential phishing.	**Supports.** Training is **out of scope**.
21(2)(h)	Policies and procedures regarding the use of cryptography and, **where appropriate**, encryption	AES-256-GCM on every tunnel. Ephemeral elliptic-curve Diffie-Hellman on NIST P-256, giving perfect forward secrecy. HKDF-SHA-512 session key derivation. ECDSA signatures over SHA-256. Replay protection through a monotonic counter and a bounded acceptance window. Payloads remain separated at intermediate hops.	**Directly addresses the technical control.** The cryptographic policy is yours to write. See the limitations section for what this suite does not carry.
21(2)(i)	**Human resources security**, access control policies and asset management	Access is granted on cryptographically verified user and device identity rather than network location. Each user and device holds its own key pair, generated on the device, with the private key never transmitted. Deletion of an identity revokes access within seconds and is recorded with the actor and the time.	**Directly addresses the access control element. Human resources security is out of scope**, and asset management is supported rather than provided.
21(2)(j)	The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems, **where appropriate**	Phishing-resistant passwordless authentication that combines a biometric check on a registered device with a private key stored in that device's keystore. There is no password to phish, reuse, or leak.	**Directly addresses the multi-factor authentication element.** Secured voice, video, text, and emergency communications are **out of scope**. Note that the Directive qualifies this entire point with "where appropriate," which leaves the judgment with you.

Article 23: Reporting, and What a Technical Control Can Contribute

The reporting clock starts when you become aware of a significant incident, not when it occurred. There are five elements, not three.

- **Early warning**, without undue delay and within 24 hours of becoming aware, indicating where applicable whether the incident is suspected to be caused by unlawful or malicious acts or could have cross-border impact.
- **Incident notification**, within 72 hours, updating the early warning and giving an initial assessment of severity and impact, with indicators of compromise where available.
- **Intermediate report**, on request from the CSIRT or competent authority.
- **Final report**, not later than one month after the incident notification, with a detailed description, the likely root cause, applied and ongoing mitigations, and cross-border impact where applicable.
- **Where the incident is still ongoing** at the point the final report would be due, a progress report at that time and a final report within one month of the incident being handled.

Qualified trust service providers report significant incidents affecting their trust services within 24 hours.

What BlastShield contributes, stated precisely.
Access records, configuration change records, and session recordings support the initial assessment at 72 hours and the root cause analysis in the final report. That is a genuine contribution to an evidence pack under time pressure.

What it does not contribute is awareness.
BlastShield does not detect incidents, so it does not start your clock. Any vendor claiming that their access control product helps you
meet the 24-hour early-warning deadline is describing a detection capability. Detection comes from monitoring, and the honest architecture pairs the two.

One practical caution on evidence.
Logs stored locally on a device rotate as storage fills up, and no retention period is guaranteed. If your incident reconstruction depends on records older than your busiest few weeks, export to a syslog destination that you size and retain. That is true of this product and of most products in the category, and it is the kind of thing discovered at the worst possible moment.

Penalties: Stated Accurately

Article 34 sets floors for the maximum fines Member States must provide and attaches them specifically to infringements of Articles 21 or 23, rather than to general non-compliance.

Essential entities
Article 34(4): administrative fines of a maximum of at least EUR 10 000 000, or of a maximum of at least 2% of total worldwide annual turnover in the preceding financial year of the undertaking, whichever is higher.

Important entities
Article 34(5): a maximum of at least EUR 7 000 000, or at least 1.4% of total worldwide annual turnover, whichever is higher.

Three points are routinely misreported. The phrase is "a maximum of at least," which sets a floor on what national law must allow, so national maxima may be higher and "fines up to EUR 10 million" understates the exposure. "Whichever is higher" means that for a large undertaking the turnover figure usually governs. And for essential entities, the temporary management ban available under Article 32(5) tends to concentrate attention more effectively than any fine.

Where BlastShield Does NOT Help

A mapping with no gaps is not credible, and an assessor will find any undisclosed gap. These are ours.

- **No detection.**
  BlastShield performs no anomaly detection, intrusion detection, behavioral analysis, or threat hunting. It constrains what sessions can exist and records them. It does not tell you that something is wrong.
- **No FIPS 140-3 validation.**
  The cryptographic suite is modern and specifiable but not validated. Where your policy or a contract requires validated cryptography, this is a gap, and it is not one that wording closes.
- **Post-quantum cryptography has not shipped.**
  It is planned for a future release. Any present-tense claim that this product supports ML-KEM or ML-DSA today would be a roadmap claim stated as fact. The previous version of this paper made that claim, and it was wrong.
- **No software bill of materials.**
  BlastWave does not currently publish an SBOM. Note also that an SBOM is not a NIS2 requirement: it appears in the Cyber Resilience Act, not in Article 21.
- **No coordinated vulnerability disclosure policy.**
  BlastWave does not currently publish one. Article 21(2)(e) concerns your vulnerability handling and disclosure, and a supplier without a disclosure policy is a reasonable thing for you to raise with us.
- **Separation of duties cannot be enforced within the product.**
  The administrative model defines two roles that apply network-wide. Separation of duties must be enforced through your own change management procedures. The product provides a complete change audit trail, which demonstrates that a procedure was followed rather than enforcing it.
- **No guaranteed log retention.**
  Local logs rotate on available storage with no set period. Retention is achieved by exporting to a destination you control.
- **No independent protocol review or penetration test report.**
  The cryptographic construction has not been reviewed externally, and no third-party penetration test report exists. We would rather tell you that than have you discover it during due diligence.
- **Most of Article 21 is organizational.**
  Risk analysis, business continuity, crisis management, supplier assessment, secure development, effectiveness assessment, training, and human resources security are program work. A product cannot do them and should not claim to.

Legacy Assets: Where This Usually Gets Difficult

The recurring obstacle to NIS2 readiness in OT is equipment that cannot be patched: controllers with a service life measured in decades, running software with published vulnerabilities and no vendor fix, which cannot be taken offline for a maintenance window because the process depends on them.

The conventional options are to physically isolate the equipment, which often means losing the connectivity that made it useful, or to place inspection hardware in front of it, which entails capital expenditure, rack space, and a change window.

A software overlay offers a third option: the asset stops responding to unauthenticated discovery and becomes reachable only after an authorized identity has been verified. The device is not modified, no agent is installed on it, and no network redesign is required. For an entity documenting its Article 21(2)(e) position on equipment it cannot patch, that is a defensible and evidenced answer.

Two honest caveats: Reducing reachability is not remediation, and the underlying vulnerability stays on your register. And protection depends on the asset's traffic passing through the enforcement point, so the design work of establishing where that is remains real work.

For Managed Service Providers

NIS2 places managed service providers and managed security service providers in Annex I, among the sectors of high criticality. An MSSP serving critical infrastructure is in scope in its own right, and its own security posture becomes part of its customers' supply chain position under Article 21(2)(d).

That creates a specific opportunity and a specific obligation. A provider that can demonstrate least-privilege, identity-based, recorded access into each customer environment, with revocation that takes effect in seconds, is answering the question its customers are now required to ask it.

Deployment and configuration are performed remotely, eliminating the need for site visits in the rollout for distributed estates.

For Equipment Manufacturers

Manufacturers of products with digital elements face obligations under the Cyber Resilience Act, a separate instrument from NIS2, with its own conformity requirements, including vulnerability disclosure and a software bill of materials. Where a manufacturer's customers are themselves NIS2 entities, the two instruments meet in the manufacturer's supply chain position.

BlastShield integrates with certified appliance platforms from OnLogic and Axiomtek and can be pre-integrated by hardware partners.

A caution on language.

"NIS2-ready" has no regulatory meaning and would not survive a procurement challenge. A manufacturer can accurately state that a product ships with identity-based access control, encrypted transport, and segmentation capabilities that support a customer's Article 21 position. It cannot say the product makes the customer compliant, because compliance is assessed against the entity, not the component.

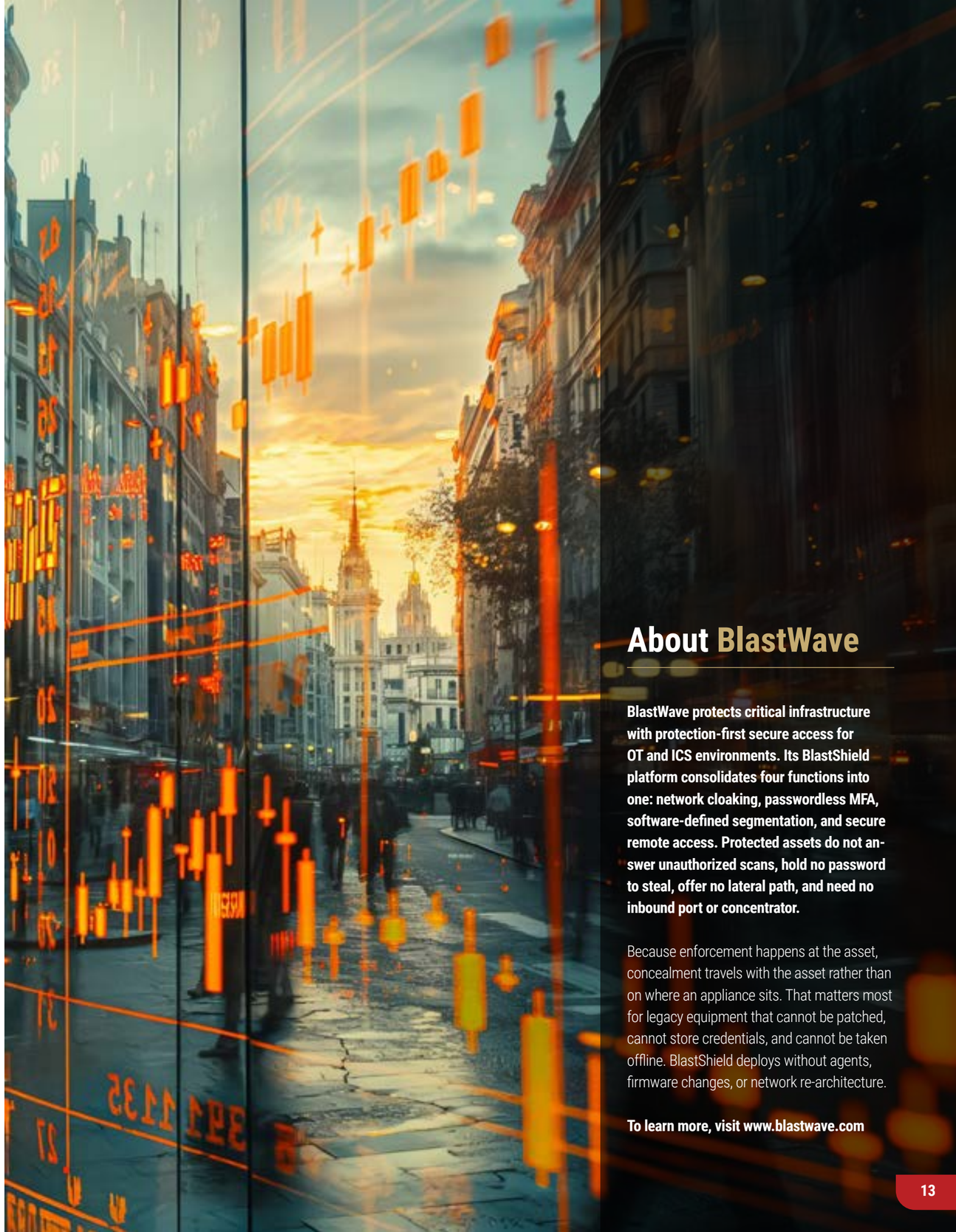
Conclusion

NIS2 is a durable shift toward evidenced, continuously operated security in European critical infrastructure, and the duties it creates fall on entities and their management bodies rather than on their suppliers.

What a software-defined perimeter changes is the cost and disruption of several controls that used to require hardware and downtime: identity-verified access that does not depend on network location, assets that do not answer unauthenticated discovery, segmentation without re-architecture, and a record of who reached what and when. Those bear on four of the ten Article 21(2) measures directly and support four more.

They do not make you compliant, and no product does. The work of policy, risk analysis, supplier assessment, continuity planning, training, and governance remains yours. A supplier worth having is one that is clear about which is which.

BlastWave



About BlastWave

BlastWave protects critical infrastructure with protection-first secure access for OT and ICS environments. Its BlastShield platform consolidates four functions into one: network cloaking, passwordless MFA, software-defined segmentation, and secure remote access. Protected assets do not answer unauthorized scans, hold no password to steal, offer no lateral path, and need no inbound port or concentrator.

Because enforcement happens at the asset, concealment travels with the asset rather than on where an appliance sits. That matters most for legacy equipment that cannot be patched, cannot store credentials, and cannot be taken offline. BlastShield deploys without agents, firmware changes, or network re-architecture.

To learn more, visit www.blastwave.com

BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to www.blastwave.com

v20260917

Prevent industrial cyberattacks, and ensure the world's critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at **www.blastwave.com**

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS