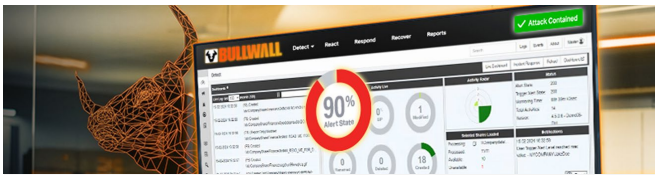




# NIS2 QUICK REFERENCE GUIDE

BullWall helps organizations with **NIS2 compliance** by providing a strong layer of **ransomware containment and incident response**, which aligns with the directive's core focus on **cyber resilience, incident detection, response, and reporting**.

Here's how BullWall contributes:



## WHAT IS BULLWALL?

BullWall offers **Ransomware Containment** technology designed to **detect and stop ongoing ransomware attacks** within seconds by quarantining infected devices and preventing file encryption from spreading across the network.

## NIS2 DIRECTIVE KEY SECURITY REQUIREMENTS

NIS2 requires organizations to:

- 1 Implement risk-based cybersecurity measures
- 2 Detect and respond to incidents effectively
- 3 Ensure business continuity during cyber incidents
- 4 Report incidents promptly (within 24 hours)
- 5 Minimize impact on essential services

## HOW BULLWALL SUPPORTS NIS2 COMPLIANCE

NIS2 Requirement	BullWall Contribution
Detection & Containment	BullWall detects live ransomware attacks <b>in real time</b> , enabling immediate containment and mitigation.
Incident Response	Automatically isolates compromised endpoints, helping to <b>limit the spread and impact</b> of attacks.
Continuity of Services	By stopping encryption in its early stages, BullWall helps maintain <b>business continuity</b> .
Post-Incident Investigation	Logs and alerts provided by BullWall assist in forensic investigations and <b>incident reporting</b> .
Minimizing Impact	Early intervention significantly reduces <b>data loss and operational disruption</b> , key goals of NIS2.
Compliance Proof / Auditing	BullWall generates <b>auditable logs and reports</b> , useful for demonstrating regulatory compliance.

## WHO NEEDS THIS?

Under NIS2, organizations in **essential and important sectors** (e.g., energy, transport, healthcare, finance, digital infrastructure) must implement strong operational security — BullWall gives them a **rapid containment safety net**.

## INTEGRATION WITH EXISTING SYSTEMS

BullWall is **agentless** and typically integrates with **existing security infrastructures (SIEM, EDR/XDR, SOAR)** to **enhance detection and response** capabilities without requiring endpoint modifications.

## FINAL TAKEAWAY

BullWall is not a full NIS2 compliance solution by itself, but it plays a **critical supporting role** in several key areas required by the directive:

- **Rapid ransomware containment**
- **Reporting and forensic support**
- **Incident response automation**
- **Reduced operational impact**

It complements your broader NIS2 compliance strategy, which would also include governance, risk management, training, and other cybersecurity controls.

## ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting data and critical IT infrastructure during active ransomware attacks. We are able to contain both known and zero-day ransomware variants in seconds, preventing both data encryption and exfiltration.

***BullWall is your last line of defense for active attacks.***

Learn more at [www.bullwall.com](http://www.bullwall.com).

