

## The AZ Monica Hospital cyber attack and Belgian threat healthcare

### Primary target

Healthcare is Belgium's most targeted sector, enduring an average of 2,620 attacks per week.

### Security gap

An estimated 75% of Belgian hospitals lack adequate cyber security defences.

### Standard compliance

Only 15% of institutions currently meet required standards for digital identification and access control.

## Incident overview

**Event:** A malicious cyber attack detected at 6:32 AM on January 13, 2026, targeting the AZ Monica Hospital network.

**Immediate action:** IT staff proactively shut down all servers across the Antwerp and Deurne campuses to contain the breach.

**Official investigation:** Confirmed as a criminal act by the Belgian Federal Police and Prosecution Service; notably, officials have refuted ransomware claims, as no ransom demand was made.

### Operational Impact

**Surgical disruptions:** Cancellation of 70+ surgical procedures and postponement of chemotherapy and radiology (MRI/CT) treatments.

**Patient safety:** Forced the transfer of seven critical care patients to other facilities with Red Cross assistance.

**Clinical paralysis:** Loss of access to Electronic Patient Records (EPR) and digital imaging, forcing staff to use manual, paper-based processes.

**Emergency services:** Emergency departments operated at reduced capacity and mobile urgency groups (MUG/ PIT) were temporarily offline.

## Government and industry response

In 2025, Belgium's healthcare sector became the country's most targeted industry, recording an average of 2,620 cyber attacks per week in Q2. This surge highlights the sector's growing exposure compared to finance and consultancy.

**Attack growth:** Healthcare incidents rose 30% year-over year.

**Sector ranking:** Ranked as Belgium's hardest-hit industry.

**Operational impact:** 16% of organisations reported disruptive attacks.

**Root causes:** Nearly 48% of ransomware stemmed from compromised VPNs. Legacy systems and the high value of medical data continue to attract 'double extortion' groups.

## Proposed framework for cyber resilience from Resillion

**Our Total Quality** framework focuses on both immediate response and long-term strategic prevention.

**Immediate incident response:** We provide a 24/7 hot-line and emergency teams for rapid containment, root-cause analysis and data exfiltration assessment to restore operations quickly.

**Digital forensics:** We use our ISO 17025 accredited labs to identify attack vectors and ensure no hidden back doors remain in the system post-incident.

**Continuous monitoring (SOC):** Our Security Operations Centre offers 24/7 monitoring to detect and block threats like ransomware before they can execute and encrypt data.

**Strategic prevention:** Services include Penetration Testing, Red Teaming and Vulnerability Monitoring to identify security gaps, particularly in access control where 85% of hospitals fail.

**Compliance & governance:** We provide CISO-as-a-Service to align hospital security practices with regulations such as NIS2, ensuring medical data remains secure and accessible.

**Ransomware readiness assessment:** Resillion can put your company's environment in a Ransomware simulation and identify further weaknesses in your systems and therefore strengthen your posture to reduce (Note: not eliminate) vulnerabilities to such attacks.



## Response and investigation summary

**Immediate containment:** Proactive shutdown of all servers at 6:32 AM to prevent further compromise.

**Patient safety focus:** Coordinated transfer of critical patients, prioritising care continuity over digital operations.

**External engagement:** Prompt notification to the Belgian Federal Police and the Antwerp Public Prosecution Service.

**Confirmed facts:** Officially classified as a malicious cyber attack, under investigation by the Computer Crime Unit.

**Key unknowns:** Perpetrator identity, motives, and whether patient data exfiltration occurred remain unclear.

**Ransomware status:** Public prosecutor confirmed no ransom demand has been made.