



BULLWALL FOR HEALTHCARE

# RANSOMWARE ATTACKS ON HEALTHCARE ORGANIZATIONS ARE ON THE RISE AND THE STAKES COULDN'T BE HIGHER

Data breaches in healthcare can result in the disruption of patient services, hefty fines for HIPAA violations, and damage to your organization's reputation. To protect against these threats, IT administrators must tackle common attack strategies like phishing emails, compromised websites, and DDoS attacks. Moreover, they face a complex cybersecurity landscape due to the growing adoption of cutting-edge medical devices and online portals, which present additional vulnerabilities for cyber criminals to access confidential health information (PHI).

## THE RISK

**328%**

Increase in healthcare ransomware attacks in the first half of 2022

**\$10.1M**

Average cost of a data breach in healthcare

**15 DAYS**

On average without access to patient records

## THE BULLWALL SOLUTION

Data security in healthcare has never been more important. Healthcare professionals find preventative solutions are no longer enough to safeguard patient information against cyber criminals. With a wide range of vulnerable entry points and innovative attack strategies, sooner or later, ransomware will slip through. That's when BullWall steps in.

***BullWall provides an automated ransomware containment solution as a proactive approach to data security, allowing healthcare organizations to detect, contain, and recover from a ransomware attack before it causes significant damage.***

The solution operates by automatically quarantining the infected users and devices, preventing the ransomware from spreading across your critical IT infrastructure and medical data – both on-premises and in the cloud. Reducing the risk of security breaches and ensuring hospitals are able to operate without a lapse in patient care.



***All healthcare organizations should deploy BullWall in my opinion. I have never seen a cyber security solution provide this level of containment and protection against ransomware attacks.***

- CIO of Irish Healthcare Organization





**DETECT**

BullWall uses 28 sensors and machine learning to monitor file activity and identify abnormal events.



**ISOLATE**

BullWall stops active attacks, quarantine the infected user & device, and protects your critical IT infrastructure.



**REPORT**

BullWall notifies your IT team within seconds and provides a report of compromised devices and files to expedite recovery.



**NO ENCRYPTION,  
NO RANSOM**

BullWall eliminates ransom demands by stopping malicious encryption in seconds.



**NO EXFILTRATION,  
NO EXTORTION**

BullWall minimizes extortion and protects PHI by preventing malicious data exfiltration.



**NO DOWNTIME,  
NO WORRIES**

BullWall thwarts and isolates attacks before the damage can spread, so there's no downtime.

**THE TRUSTED PARTNER IN HEALTHCARE DATA SECURITY**

BullWall is currently protecting over 70,000+ healthcare professionals around the world, enabling organizations to:

- ✓ Prevent healthcare data breaches
- ✓ Stop the exfiltration of PHI and PII
- ✓ Protect EMR/EHR systems and IT infrastructure
- ✓ Ensure continuity of healthcare services
- ✓ Generate HIPAA data breach reporting



**THE ONLY SOLUTION OF ITS KIND**

BullWall is designed to be easy to implement and operate, enabling healthcare organizations to respond quickly to an attack and reduce downtime. Entirely automated, the system requires no hands-on monitoring and can be integrated with your other security solutions.

**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).

