BULLWALL FOR HEALTHCARE

In recent years, ransomware attacks have severely impacted the healthcare sector, with over 500 successful attacks compromising the records of more than 52 million patients.

THE CONSEQUENCES OF RANSOMWARE ATTACKS IN HEALTHCARE REACH FAR BEYOND THE BILLIONS IN FINANCIAL DEVASTATION.

As healthcare organizations struggle with rising cyber insurance costs and insufficient recovery strategies, patient care suffers or ceases altogether. The need for rapid containment and response is more urgent than ever.

WHY BULLWALL?

BullWall directly prevents and contains ransomware, ensuring that healthcare providers can maintain operational continuity, protect sensitive data, and minimize risks to patient care when ransomware strikes.

66%

of ransomware attacks
disrupted patient care

46%

of respondents reported
increased mortality rates

The Impact of Ransomware on Patient Safety and the Value of Cybersecurity Benchmarking, Proofpoint

> *Prevention alone is no longer enough.* ***Ransomware has advanced, and healthcare is a prime target.*** *It's critical to focus on how quickly you can contain an attack once it breaks through to reduce patient care impact and be resilient.*

JAMES CASE
VP & CISO Baptist Health

HOW HEALTHCARE BECOMES A RANSOMWARE TARGET

BYPASSING DEFENSES

68%

of ransomware attacks in healthcare were caused by compromised credentials, often involving social engineering or vulnerabilities in medical systems like EHRs and diagnostic tools.

UNPATCHED SYSTEMS

83%

of healthcare organizations use legacy IT systems that can't be easily updated or patched, leaving critical patient data and operational systems vulnerable to cyberattack.

EXPANDED ATTACK SURFACE

41%

of ransomware attacks in healthcare exploit vulnerabilities in medical devices or connected systems, which provide multiple entry points for cybercriminals.

THE IMPACT

In recent years, ransomware attacks have severely impacted the healthcare sector, with over 500 successful attacks compromising the records of more than 52 million patients.

PATIENT CARE IMPACT

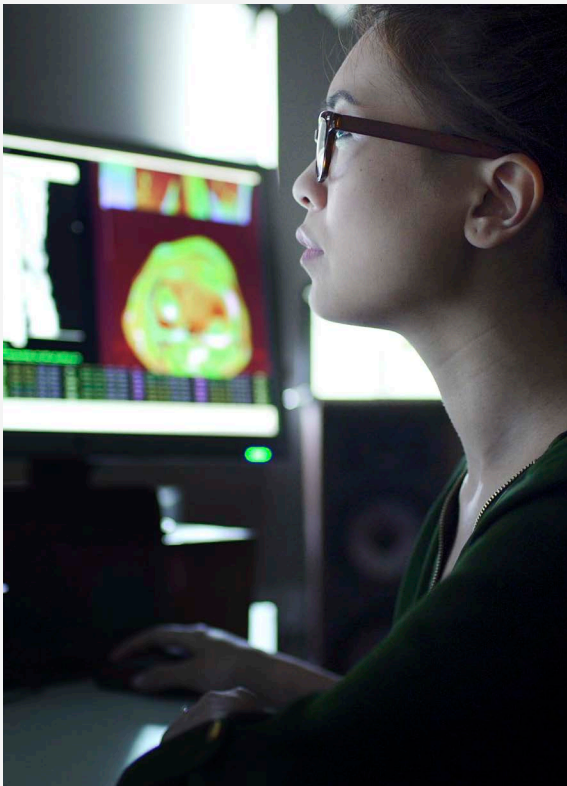
Critical IT systems like electronic health records (EHR), medical equipment, and operating rooms can be locked, leading to treatment delays, cancellations, and misdiagnoses.

EXPOSED PATIENT DATA

Cybercriminals exploit patient data for profit, leaving individuals feeling exposed and betrayed by the very healthcare providers entrusted with their care.

FINANCIAL & OPERATIONAL IMPACT

Ransomware attacks can cripple healthcare networks for an average of 21 days, costing up to $10.1 million in ransom payments, recovery costs, operational downtime, and HIPAA-related fines. Healthcare providers that contain and recover from an attack within 24 hours have historically reduced their financial impact by 50%.



WHAT IS RANSOMWARE RESILIENCE?

Ransomware resilience is the ability to prevent, contain, and respond to ransomware attacks, minimizing damage and ensuring rapid recovery of data and operations to maintain business continuity.

PREVENTION

Reduce the risk of disruptions to operations, which can be costly and damaging to productivity.

CONTAINMENT

Minimize the impact to business operations when ransomware gets through, and significantly reduce recovery efforts.

RECOVERY

Resilient organizations recover quickly to limit operational downtime and return stronger.

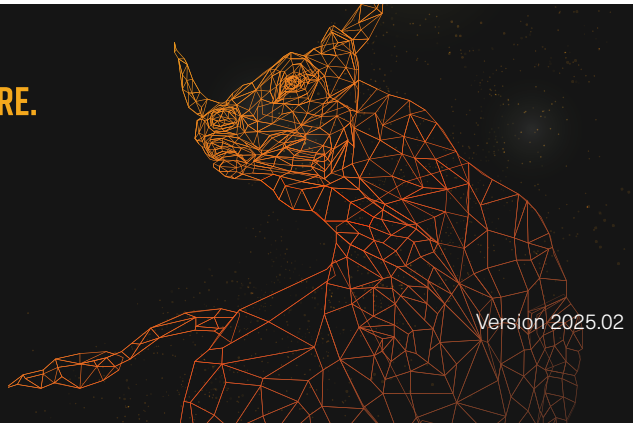
BE RANSOMWARE READY... WITH BULLWALL

BullWall's unique approach to ransomware provides server-based protection without an endpoint agent to secure critical IT infrastructure and maintain operational continuity across all stages of an attack—before, during, and after.

Legacy IT systems are easy targets for ransomware.	**BullWall is the only solution that immediately contains an active attack,** preventing spread, protecting patient data and critical operations, even on outdated infrastructure.
Ransomware exploits weaknesses in systems like EHRs and diagnostic tools.	**BullWall addresses urgent gaps left by traditional security solutions,** containing attacks instantly without endpoint installations, ensuring healthcare systems stay secure.
Medical devices, BYOD, and patient data systems offer multiple entry points for ransomware.	**BullWall protects all data and critical IT infrastructure,** safeguarding vulnerable systems and preventing attacks from reaching vital infrastructure.

THINK YOU'RE RANSOMWARE RESILIENT? FIND OUT FOR SURE.

BOOK ASSESSMENT



BULLWALL | RANSOMWARE RESILIENCE FOR CRITICAL IT INFRASTRUCTURE