BULLWALL FOR ALL

Organizations across all industries are prime targets for ransomware attacks. Between 2018 and 2023, businesses and institutions worldwide faced significant financial losses, with downtime costs reaching hundreds of millions due to ransomware incidents.

A SUCCESSFUL RANSOMWARE ATTACK CAN HAVE GRAVE CONSEQUENCES THAT REACH FAR BEYOND THE FINANCIAL IMPACT.

From disrupting essential operations, such as financial transactions and customer services, to halting critical infrastructure and compromising sensitive data, the urgency to prevent and mitigate ransomware attacks has never been greater.

WHY BULLWALL?

BullWall offers a specialized ransomware containment solution that safeguards organizations across all industries by rapidly detecting and stopping ransomware attacks before data can be encrypted or exfiltrated.

By halting attacks in real time, BullWall helps organizations prevent data breaches that could expose sensitive information, disrupt critical operations, and compromise essential systems across various industries.

66%

of organizations reported being **victims of ransomware attacks** in 2023

$1.85M

average cost of an attack in 2024 encompassing expenses related to downtime, recovery, and potential ransom payments

Sophos State of Ransomware Report

> ***Ransomware resilience is now essential.*** *Cybersecurity teams must be ready to contain and recover swiftly, recognizing that blocking every threat is no longer possible.*
>
> **BRIAN MURPHY**
> Head of Cybersecurity at MJ Flood Technology

HOW ORGANIZATIONS BECOME A RANSOMWARE TARGET

PHISHING EMAILS

41%

of ransomware attacks are caused by phishing, the most common entry point.

UNPATCHED SOFTWARE & VULNERABILITIES

30%

of ransomware attacks are caused by unpatched vulnerabilities.

COMPROMISED REMOTE DESKTOP PROTOCOL (RDP)

25%

of ransomware incidents are the result of RDP compromises.

THE IMPACT

The impact of an attack far outweighs the simple financial loss of paying the ransom. Many other factors must be considered, all of which have long-lasting implications for the future of the affected organization.

CRITICAL DATA EXPOSURE & OPERATIONAL DISRUPTION

A ransomware attack that compromises sensitive data can violate industry and regulatory data protection laws, such as GDPR, HIPAA, and other compliance frameworks specific to the affected sector.

DISRUPTION OF BUSINESS-CRITICAL SYSTEMS

A ransomware attack can severely disrupt business-critical systems, halting essential operations and causing significant downtime. By encrypting key infrastructure and demanding ransom for restoration, attackers can paralyze supply chains, disrupt production lines, and prevent access to vital data and services—leading to financial losses, operational delays, and reputational damage.

IMPACT ON EMPLOYEES AND SUPPLIERS

A ransomware attack can severely impact employees and suppliers by disrupting daily operations and access to critical systems. Employees may face downtime, making completing tasks, communicating, or accessing vital company resources difficult, leading to frustration and productivity loss. Suppliers could experience delays in receiving or delivering goods and services due to compromised systems, affecting relationships and supply chain efficiency. In the long term, these disruptions can damage business partnerships, erode trust, and harm the overall financial stability of the organization.

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.

Phishing emails are the preferred method of delivery for cybercriminals.	**BullWall is the only solution that immediately contains an active attack** regardless of the delivery method, ensuring resilience and business continuity.
Unpatched software and existing vulnerabilities within organizational systems provide cybercriminals with easy access to your network.	**BullWall protects you from both known vulnerabilities and hidden threats** you may not even be aware of.
Cybercriminals often disable preventative security solutions before launching an attack, with compromised Remote Desktop Protocol (RDP) sessions being their preferred method of entry.	**BullWall Server Intrusion Protection stops this breach risk** and enhances ransomware resilience by securing remote server access and critical server

ABOUT BULLWALL

BullWall is the pioneer in ransomware resilience, providing robust defenses against the relentless threat of ransomware.

Learn more at www.bullwall.com.

BULLWALL