



BULLWALL FOR GOVERNMENT

RANSOMWARE ATTACKS CAN CRIPPLE GOVERNMENT INSTITUTIONS LEADING TO THE DISRUPTION OF ESSENTIAL SERVICES



More than 70% of government institutions reported a ransomware attack in 2023 with these attacks coming not only from professional ransomware gangs, but also state sponsored bad actors looking to cause wide spread disruption to public services and critical infrastructure. While government agencies understand the issue and are making strides to stop attacks, these are becoming ever more sophisticated with the use of Zero Day exploits and artificial intelligence.

THE RISK

70%

of local and federal government institutions reported a ransomware

\$3.9M

Average cost of ransomware payout in government sector

45,000

files disrupted on average per attack

THE BULLWALL SOLUTION

Ransomware is now the greatest cyber and organized crime threat to local and national critical infrastructure. The significant impact on victims due to financial, data and service losses, which can lead to business closure, inaccessible public services and compromised customer data cannot be underestimated or ignored. BullWall provides a last line of defense designed to stop ransomware once it has bypassed traditional preventative measures.

The solution leverages 28 detection sensors and machine-learning capabilities to instantly detect illegitimate encryption and exfiltration. Once detected the solution immediately and automatically activates an isolation and containment protocol for compromised users and devices initiating abnormal encryption, stopping the attack in its tracks with minimal disruption.



We cannot take our eyes off the ball, and BullWall Ransomware Containment has given us the additional eyes to help tackle this type of activity.

- IT Manager of Large UK Council





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 PII 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 GOVERNMENT DATA SECURITY

BullWall is currently protecting over 130,000+ government employees around the world, enabling them to:

- ✓ Prevent data breaches
- ✓ Stop the exfiltration of information
- ✓ Safeguard essential services
- ✓ Maintain public safety



THE ONLY SOLUTION OF ITS KIND

BullWall is designed as a lightweight, agentless solution that is easy to implement and operate allowing government institutions to automate their ransomware protection for 24/7 coverage. The system integrates with the other solutions in your security stack and requires no hands-on monitoring, ideal for organizations of all sizes.

ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting critical IT infrastructure from ransomware. We provide rapid containment of active attacks, and safeguard servers by preventing unauthorized intrusion.

Learn more at www.bullwall.com.

