
STOP RANSOMWARE BEFORE IT STOPS YOU -Click to watch the video

**BullWall's RansomCare (RC)** is the Last Line of Defense to detect and stop active ransomwar e encryptions within file shares and servers by isolating compromised users and devices; protecting busines esential data and preventing operational downtime.

Most organizations have already invested and implemented strong layers of security but are still vulnerable to ransomware. Cybercriminals are constantly outsmarting even the most robust security solutions. They rapidly evolve their methods and behaviors, making it impossible for traditional security vendors to prevent them. Relying on existing endpoint protection is no longer enough. Ransomware can encrypt **20,000** files per minute: costing companies on average **$1.5 million** per attack.

RC is the ***only*** solution focused on the file level, the unprotected area, to minimize ransomware outbreaks instead of attempting to recognize and prevent all malware. With over 500 organizations protected by RC globally, our agentless solution is trusted to be the most reliable containment tool to reduce ransomware devastation.


*51% of malware strains surpassing existing security solutions.*

## The *ONLY* reliable solution to the costly and inevitable cyber threat...

RC does not depend on outdated detection methods such as ransomware signatures, strains, patterns, or behavior. Instead, RC rapidly detects the malicious actions of the ransomware - file encryption. It does so without any network overhead or performance degradation. RC differentiates by monitoring the activity on file shares, application servers, and database servers.

Through machine learning, RC analyzes file activity and uses research-based detection sensors to recognize threats- regardless of the file type or activity; whether the file is renamed, modified, created, or deleted. Once RC detects malicious encryption, it isolates any compromised user(s) or device(s) within seconds, preventing substantial damage to file shares and financial implications.

* Response to attacks is customizable- i.e., powering down a compromised machine, disabling the user in the cloud or Active Directory, revoking SMB permissions, disabling VPN sessions, etc.

## Complement and enhance existing security infrastructure...

RC integrates with your existing security stack (ITAM, SIEM, EDR, NAC) via RESTful Web APIs and works in parallel with vendors such as Carbon Black, CrowdStrike, McAfee, Symantec, SentinelOne, Sophos, and many more- adding an additional layer of protection and strengthening the value of your existing cyber security structure. RC is fully scalable from a local singular institution to a large school district, no matter the size of the current IT infrastructure or the type of file applications used.

## RC delivers the ultimate ransomware defense for any budget...

RC repeatedly proves itself to prevent the worst-case scenario, acting as a vital Last Line of Defense, mitigating long-term damage, disruption, and cost of active ransomware attacks... **RC detects when others fail to protect.**

## See it for yourself

**Experience BullWall's live demonstration**

**Learn about the ransomware assessment**

**Concerned about ransomware?** Book live demonstration or assessment on **bullwall.com**

Version 2 | 二版
www.version-2.com
Hong Kong | Taiwan | Singapore | Macau | Mainland China

**Hong Kong & Macau**
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

**Taiwan**
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

**Singapore & SEA**
Tel : (65) 6296 4268
Email : sales@version-2.com.sg