The RansomCare offering is an automated containment solution, laser-focused to stop malicious encryption and file corruption on monitored file shares, securing critical data.

Let's face facts: Even the most well-protected organizations fall victim to ransomware. Cyber criminals are constantly developing new and innovative methods to defeat traditional, prevention-based detection methods.

A recent G7 report stated: *"Companies need to move beyond traditional perimeter security to defend against ransomware, by employing layered security to prevent, detect, and remediate malicious activity that may be conducted within the network."*

To mitigate the ransomware risk, an organization must follow G7's recommendations and evolve its security defenses by introducing a layered approach. Once ransomware has breached the network and begins delivery of its payload, it's too late for existing security to react. At this point, the only thing that matters is how fast you can stop the illegitimate encryption from encrypting up to 10,000 files per minute.

BullWall's multi-layered containment solution, RansomCare (RC), detects and reacts to malicious file corruption and encryption, and stops it in its tracks. The solution is agentless and utilizes more than 20 detection sensors to detect the tell-tale signs of active ransomware. If malicious encryption is initiated by a compromised user or files are corrupted on monitored file shares, RC reacts by isolating the compromised device and user to stop the illegitimate encryption process.

RC is complementary to existing security defenses. Where traditional security defenses focus on preventing malware from executing and protecting your organization, they are not sufficient against ransomware. It has crippled organizations even though they had the best-of-breed security solution in place.

Organizations should consider deploying a Last Line of Defense acting as the sprinkler should malicious encryption be active. RC reacts once malicious file encryption and/or file corruption is ongoing on monitored critical file- and cloud shares (e.g. Google and O365). It is crucial during ransomware outbreaks to detect, respond and recover as quickly as possible, as the financial and reputational repercussions caused by downtime can be costly.

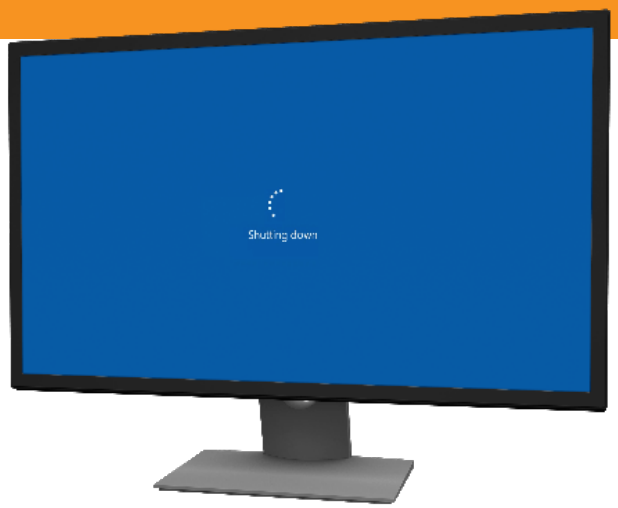
We are very proud to serve customers in all industries, including the financial sector, education, healthcare, legal and manufacturing. Our customers state that RC has procured via Sole Sourcing (US) and on Exceptions Documentation (UK), proving its uniqueness.

KEY HIGHLIGHTS

- **A proven, 24/7 automated response**
- **Agentless: Hassle-free deployment**
- **No network or performance overhead**

BullWall A/S • Oester Snedevej 15 • 7120 Vejle East • Denmark | BullWall Ltd • 8 The Courtyard • Furlong Road • Bourne End • Bucks SL8 5AU • England

RC is considered a Last Line of Defense technology; it detects illegitimate file encryption in seconds when all other security solutions have failed to protect your organization.



DETECT: DETAILED LIVE VISIBILITY

RC detects illegitimate encryption on monitored file shares in seconds by monitoring the organization's data activity. RC investigates the heuristics of each file accessed by a user either on-premise or in the cloud, without any network overhead.

By intelligently accumulating any detection of tell-tale signs of ransomware (encryption), RC will detect and respond to the active threat that existing security defenses did not stop.

Machine Learning automates the initial alert settings based on your actual data activity, tailoring them to your environment. Organizations are often astonished by the detailed overview of the file changes within their organization, and in case of an outbreak, you can see the small number of files impacted before the forced isolation by RC.

RESPOND: STOP THE OUTBREAK

On detecting illegitimate encryption, RC immediately raises an alert, and a response is triggered to isolate the endpoint, device and/or user that is causing the illegitimate encryption on monitored file shares.

A wide range of customizable isolation methods can be utilized, such as forced shutdown, disable VPN, disable AD-user, disable network access, and many others.

Alerting is done via email, text, and through easy integration with all SIEM solutions. The alerting also works if you are hosting in the cloud or have an MSP taking care of your IT infrastructure.

Integration through RESTful API to other security solutions means your security teams can unify security management across an increasingly complex sea of endpoints.

RECOVER: PROVIDES THE FULL OVERVIEW

RC provides a speedy data recovery concept. It provides a detailed list for restoring purposes of the small number of affected files before the forced isolation or shutdown. This reduces potential downtime significantly as it identifies the exact small number of files that need to be recovered, saving you valuable time with minimal recovery cost.

HASSLE-FREE INSTALLATION

RC is an agentless solution and is not installed on endpoints or any existing servers or file servers. There is no impact on endpoints and no network performance issues. Agentless file behavior monitoring and machine learning techniques are deployed with ease in less than a day, and RC will configure automatically.

NEXT STEPS

Learn more on bullwall.com; here, you can see a video demonstration of RC. You can also book an online demo and/or a two-hour Ransomware Assessment. During the Assessment, we utilize our safe and controlled ransomware simulator for you to experience RC at work in your own environment. You can also test your existing security defenses response to zero-day encryption, known signatures and rapid file changes on file shares.

BullWall A/S • Oester Snedevej 15 • 7120 Vejle East • Denmark | BullWall Ltd • 8 The Courtyard • Furlong Road • Bourne End • Bucks SL8 5AU • England