# Ransomware Assessment Test

In the past six months, we have seen a significant number of organizations fall victim to ransomware outbreaks. Despite having the best prevention-based solutions that money can buy, these solutions stood no chance when just one user or device was compromised and began to encrypt up to 10,000 files per minute. Ransomware is the most damaging, disruptive, and costly form of malware to hit organizations today. The financial and reputational impact is very high – and paying the ransom will incentivize the criminals to carry out more attacks.

To assist organizations in the battle against ransomware criminals, we offer a non-obligatory Ransomware Assessment Test. This assessment conducted by our Cyber Security Experts will test your current infrastructure resilience against a ransomware outbreak. The assessment takes just two hours and is conducted in a completely safe and controlled manner. We have a brief list of prerequisites for you to prepare within your security environment.

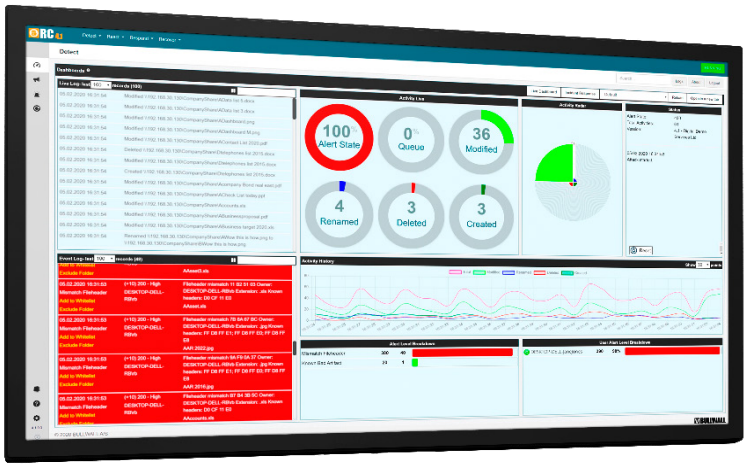
## Test your current defences

The process is straightforward. You will need to stand up a virtual server and follow a short prerequisites document we will forward to you. The preparation will take your IT-department approximately 30 minutes. This should be done in advance of the date of the assessment. On the agreed day - we do a Teams or TeamViewer session with your organizations and install and configure our new RansomCare offering. After that, we carry out the assessment that consists of three different encryption simulations.

We regularly conduct ransomware assessments up against environments running Antivirus, Next-gen Antivirus, and EDR solutions – the best-of-breed solutions are all robust from a prevention perspective – yet the hundreds of assessments we have conducted have shown us that many cannot stop ongoing illegitimate encryption.

**If you cannot answer these questions, we would recommend an assessment:**

- **How do you identify which user and which device initiated the outbreak (Patient Zero)?**
- **How do you stop the ongoing encryption immediately before significant damage occurs?**
- **How do you see which files are encrypted and where they reside?**




We offer this assessment test in conjunction with a short demonstration of our RansomCare offering. Our innovative and agentless solution, RC, is a new Last Line of Defence technology that detects Ransomware outbreaks in seconds by monitoring the organisation's data activity. RC investigates the heuristics of each file accessed by a user either on-premise or in the cloud, without causing any network overhead.

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