A two-hour investment of time will provide you with a clear view of your current security posture by testing RansomCare in your environment and testing your infrastructures response against active ransomware behavior.

Let's face facts: Even the most well-protected organizations fall victim to ransomware. Cybercriminals are constantly developing new and innovative methods to defeat traditional, prevention-based detection methods. BullWall's multi-layered containment solution, RansomCare (RC), detects and reacts to malicious file corruption and encryption and stops it in its tracks.

To help organizations better understand the objective of a Last Line of Defense solution, BullWall offers a no-obligation Ransomware Assessment Test. During the assessment, the Assessment App tool is utilized. The Assessment App is built to simulate ransomware behavior on file shares and includes a range of simulations, including zero-day file encryption, active file corruption, ransom notes, known-bad signatures, and more. The tool is safe and controlled, and all ransomware worm capabilities have been removed.

WHAT IS A RANSOMWARE ASSESSMENT TEST?

It is an online and remote two-hour session that requires one hour of preparation in advance by your IT team. The assessment will help you understand your resilience to an outbreak of malicious encryption and file corruption on your file shares, typically caused by a ransomware attack.
A simple list of pre-requisites will be shared that should be completed before the session. In preparation, you are asked to prepare a virtual server with light specs, set up a service account, and test a client with access to a demo share. The Ransomware Assessment Test is an entirely remote process, typically via Microsoft Teams and TeamViewer. RC will be installed as part of the test.

~1.5 hours
1-2 IT Professionals
Technical Configuration

~30 minutes
All interested
Assessment Session

On the agreed date, a BullWall Engineer and 1-2 of your operational or technical resources will spend approx. 1.5 hours completing the technical configuration before the assessment. After the configuration, the approx. 30-minute assessment will begin. You can share the invite with a broader group of attendees and interested stakeholders; they will be called in once configuration is over and the assessment begins.

RANSOMWARE BEHAVIOR ON YOUR FILE SHARES

Test #1: In the first test, we test a scenario where a device is not running active AV/EDR security or where ransomware has disabled the AV/EDR service agents running on the test client. In this *worse case scenario*, we test what the next reaction point is in your security infrastructure when ransomware behavior is active on your file shares.

Test #2: In the second test, RansomCare is enabled, and the selected simulations are re-run. The scenario is the same; a user is compromised, but now the RansomCare (RC) solution is monitoring the file shares.

Test #3 (Optional): In the third and optional test, you can enable and test your existing security defense's (e.g., EDR, AV) response to the ransomware simulations. Here you can also experience how well RC complements your existing tools.

Suppose ransomware is active on your data storage. Consider the following:

- How do you identify which user and which device is causing the encryption (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?

The assessment will bring you answers to those questions.

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