BULLWALL

# BULLWALL'S COMPLIMENTARY RANSOMWARE ASSESSMENT SIMULATES REAL-LIFE ATTACKS

Cybercriminals constantly develop new and innovative methods to circumvent prevention-based security tools, causing even the most well-protected organizations to fall victim to ransomware. To determine if an organization is vulnerable to modern-day ransomware attacks, BullWall offers a complimentary Ransomware Assessment to evaluate the existing security infrastructure's active response.

## WHAT IS BULLWALL'S RANSOMWARE ASSESSMENT?

The Ransomware Assessment is a penetration test (pentest) conducted remotely with a designated BullWall Security Expert to evaluate an organization's existing data and cyber resilience. A BullWall Security Expert will conduct numerous real-life ransomware simulations in a safe and controlled manner. This pentest will demonstrate malicious activity within data shares and critical IT infrastructures.

**1,700** The number of Ransomware Assessments conducted by BullWall.

**99%** Percentage of security environments that failed to detect ransomware.

**100%** *Percentage of customers benefitted from* adding a ransomware containment solution to their environment.

## PREPARATION

Your IT team is provided a list of prerequisites, which takes approximately 1 hour. These prerequisites include creating a virtual server with light specs, a service account, and a test user with access to the file share. This is completed before meeting with the BullWall team for the pentest.

## CONFIGURATION

The initial 1.5-hour meeting will occur between a BullWall Security Expert and your IT administration team to complete setup and configuration.

## THE SIMULATION

Once the initial configuration is complete, a 30-minute Ransomware Assessment will be conducted by a designated BullWall Security Expert. During this time, you can can invite additional stakeholders and decision-makers.

PART A: The Security Expert will simulate various ransomware attacks in the existing security environment to assess how current tools respond to file encryption activity within the dedicated file share.

PART B: The Security Expert will simulate the same ransomware attacks with BullWall RansomCare enabled to demonstrate isolation protocol when encryption activity is detected.

**Suppose ransomware circumvented perimeter protection tools; consider the following:**

- How would you identify which user and device is causing the encryption (Patient Zero)?
- How would you stop the ongoing encryption before significant damage occurs?
- How would you determine which files are encrypted and their locations?

**BullWall's Ransomware Assesment will demonstrate how to answer these questions.**

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