BULLWALL
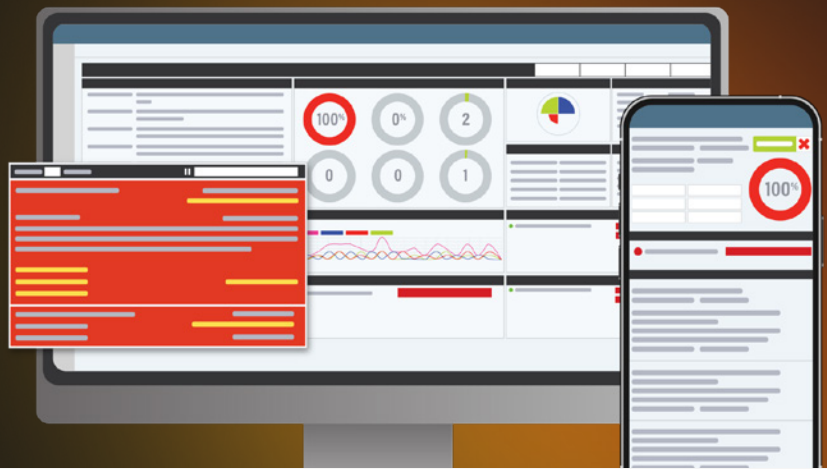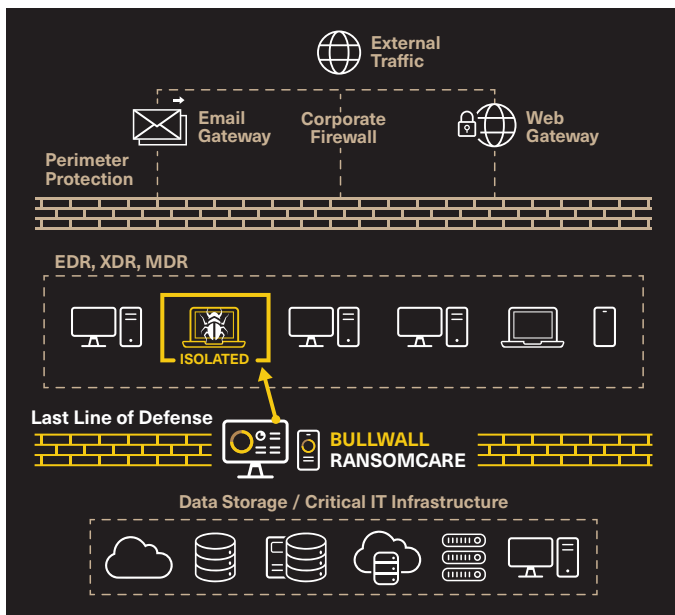
RANSOMCARE
THE RANSOMWARE KILL SWITCH

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; evolving methods and behaviors make it impossible for traditional security vendors to prevent them. *Endpoint protection is no longer enough.*

BullWall RansomCare is an active defense that stops ransomware attacks within data shares and critical IT infrastructure by automatically isolating compromised users and devices, protecting business essential data and preventing operational downtime.

THE RANSOMWARE CONTAINMENT LAYER YOU NEED.

RansomCare detects and responds the very second illegitimate encryption begins. BullWall RansomCare 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.

THE ONLY RELIABLE SOLUTION TO THE COSTLY AND INEVITABLE CYBER THREAT.

BullWall does not depend on outdated detection methods such as ransomware signatures, strains, patterns, or behavior.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

Agentless & Easy to Implement
Nothing to Install on Endpoints

Protects All Critical IT Infrastructure

Automated Compliance Reporting for Standards
Such as GDPR or NIST

24x7 Automated Detection and Response

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

COMPLEMENT AND ENHANCE EXISTING SECURITY INFRASTRUCTURE

BullWall integrates with your existing security stack (ITSM, 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 existing cyber security layers. BullWall is fully scalable from a small business to a large global enterprise, no matter the size of the IT infrastructure or the type of file applications used.

BullWall repeatedly proves itself to prevent the worst-case scenario, acting as a vital layer of defense, mitigating long-term damage, disruption, and cost of active ransomware attacks.

BULLWALL

AGENTLESS
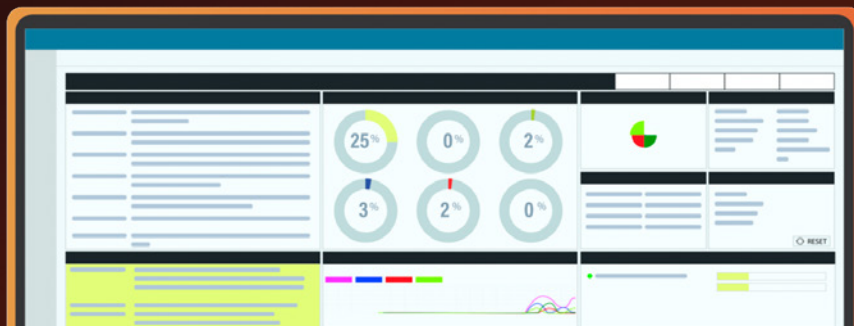
LIGHTWEIGHT

EASY SET UP

ENTIRELY AUTOMATED

NEEDS NO MONITORING

INTEGRATES WITH SIEM, NAC, EDR...

RANSOMCARE PROTECTION

1

Monitor & Detect

Monitor data activity in real-time on *SAN/NAS file shares*, VMs, domain controllers, database servers and application servers, on-prem and in the cloud.

Leverage 28 detection sensors and machine-learning capabilities, instantly detect illegitimate encryption and exfiltration.

2

Isolate & Quarantine

Immediately and automatically activate an isolation and containment protocol for compromised users and devices initiating abnormal encryption.

Deploy built-in scripts to stop file encryption and data exfiltration in seconds.

Alert IT through a built-in dashboard, email, SMS, app, or integration with SIEM, NAC, EDR and other security solutions via RESTful API.

3

Recover & Report

Quickly identify any encrypted files that can be restored from backup.

Fully automate compliance incident reporting with an advanced history log that captures all attack details, suitable for internal leadership and external government agencies.

INTEGRATION WITH THE WORLD'S LEADING SECURITY SOLUTIONS

splunk>   IBM QRadar   RAPID7   CISCO   Windows Defender ATP

LogRhythm   CROWDSTRIKE   TREND MICRO   ForeScout   Symantec by Broadcom Software

Today's ransomware is capable of encrypting up to 25,000 files per minute per infected machine.

ONLY BULLWALL CAN STOP IT

ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting data and critical IT infrastructure during active ransomware attacks. We are able to contain both known and zero-day ransomware variants in seconds, preventing both data encryption and exfiltration.

BullWall is your last line of defense for active attacks.

Learn more at www.bullwall.com.

BULLWALL

Version 2023.04