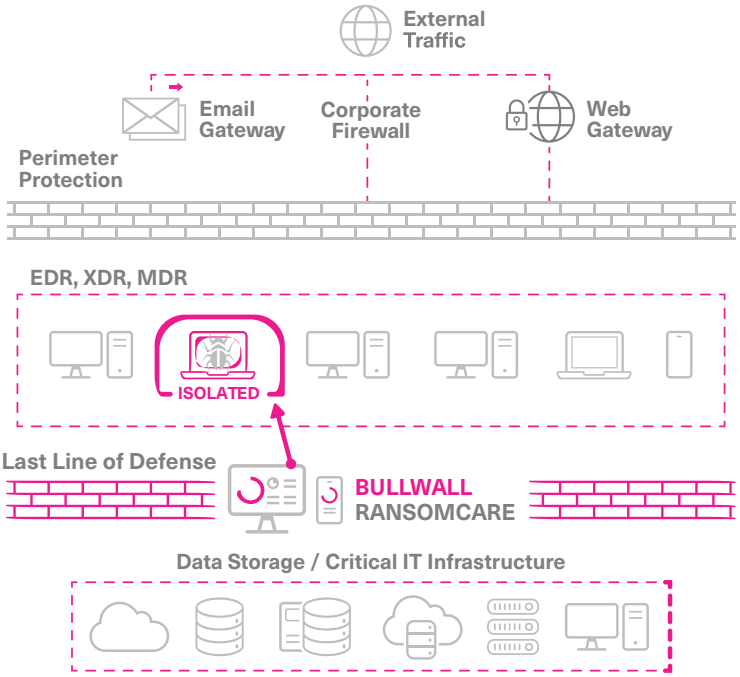
PRODUCT BRIEF

RansomCare

The Ransomware Kill Switch

Most organisations 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 behaviours make it impossible for traditional security vendors to prevent them. Endpoint protection is no longer enough.

Viatel RansomCare by Bullwall is an active defence 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 minimise ransomware outbreaks instead of attempting to recognise 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BullWall does not depend on outdated detection methods such as ransomware signatures, strains, patterns, or behaviour. Instead, BullWall rapidly detects the malicious actions of the ransomware: fi le encryption. It does so without any network overhead or performance degradation. It differentiates by monitoring the activity on fi le shares, application servers, and database servers.

Contact us today about Viatel Ransomware

hello@viatel.com

www.viatel.com

Easy to Implement

- Nothing to Install on Endpoints
- Protects All Critical IT Infrastructure 24x7
- Automated Detection and Response
- Automated Compliance Reporting for Standards such as GDPR or NIST

Corporate Firewall

- Isolated
- EDR, XDR, MDR
- Data Storage / Critical IT Infrastructure
- Perimeter Protection
- Email Gateway
- External Traffic
- Web Gateway

Last Line of Defence

Most organisations 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 behaviours make it impossible for traditional security vendors to prevent them. Endpoint protection is no longer enough.

Agentless

- Entirely Automated
- Lightweight
- Needs No Monitoring
- Easy Set Up
- Integrates with SIEM, NAC, EDR

Through machine learning, BullWall analyses file activity and uses research-based detection sensors to recognise 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 cybersecurity 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 defence, mitigating long-term damage, disruption, and cost of active ransomware attacks.

Viatel & Bullwall: A Trusted Partnership

At Viatel, we are proud to work with world-leading partners to deliver state of the art managed security solutions to our customers. Our unparalleled cybersecurity expertise enables us to deploy Bullwall's robust ransomware seamlessly, so you can be rest assured that your business is in safe hands. Learn more at **www.viatel.com.**

BULLWALL

Integration with the World's Leading Security Solutions

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.

splunk> IBM QRadar

LogRhythm CROWDSTRIKE

RAPID7 CISCO

TREND MICRO ForeScout

Windows Defender ATP Symantec. by Broadcom Software

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

Only Viatel RansomCare by Bullwall stop it.