RICOH
imagine. change.

Ransomware containment

Contain ransomware outbreaks and mitigate damage with a last line of defence.

Every day, the frequency and sophistication of ransomware attacks is climbing and is predicted to cost victims billions annually by 2031, with a new attack on businesses or consumers every 2 seconds.[1] To stay ahead of ransomware, prevention-based detection methods are no longer enough — businesses need a multilayered approach that includes endpoint protection to stop a ransomware outbreak in its tracks when other security solutions fail.

BullWall Ransomware Containment is an agentless solution that proactively monitors traffic across endpoints, file shares, and servers both on-premises and in the cloud to quickly detect any signs of a ransomware breach. It is designed to stop ransomware attacks, even when the malware has bypassed all your existing endpoint protection, and other prevention or behavioural security tools.

Ransomware Containment can identify both known and unknown variants of ransomware and doesn't rely on specific signatures or malware definitions, making it highly effective against constantly evolving threats. With its agentless approach, it is easily deployed and can be seamlessly integrated with your current security solutions to provide critical security protection for your business.

Can you answer these questions in the event of a ransomware outbreak?

- Can you see which files are encrypted and where they reside?
- Can you identify which user and which device initiated the attack?
- How do you stop the ongoing encryption immediately before significant damage occurs?
- What is the total cost of downtime as you restore hundreds of thousands of files?

[1] Cyber Magazine: Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. July 2023.

How BullWall Ransomware Containment works

With a rapidly expanding attack surface and multiple entry points for malware, Ransomware Containment provides a 24/7 automated containment response to ransomware outbreaks, with built-in response and reporting that shows the exact files infected.

The source of the attack, whether it's a user, device, or the type of ransomware, doesn't matter. Ransomware Containment is equipped to handle various attack origins, whether it's endpoints, mobile phones, IoT devices, email, website drive-by-attacks, instant messaging apps, USB keys, downloads, or internal deployments within your organization. It is equipped to handle various attack origins, whether it's endpoints, mobile phones, IoT devices, email, website drive-by-attacks, instant messaging apps, USB keys, downloads, or internal deployments within your organization.

When Ransomware Containment detects a ransomware attack, an instant alert is raised, and a response can be triggered to shut down the affected endpoint (Windows, Mac, and Linux), halting encryption immediately. It also extends its protection to virtual environments like Citrix servers/sessions, terminal servers/sessions, Hyper-V, VMware, and cloud platforms including Azure, Amazon AWS/EC2, SharePoint, Google Drive, and Microsoft 365. Mobile devices are also covered as BullWall Ransomware Containment effectively disables and stops the encryption of your data.

Hassle free remote installation

Ransomware Containment is an agentless solution, meaning it is not installed on endpoints or any existing servers. Therefore, it can't impact your endpoints or cause any network performance issues. With agentless file behaviour monitoring and machine learning techniques, deployment takes only 4 to 6 hours, and is configured automatically.

Additionally, Ransomware Containment offers seamless integration with other security solutions, such as Cisco ISE, Windows Defender ATP, SIEM systems through RESTful API and more. This integration empowers your security teams to unify security management across an increasingly complex range of endpoints.

- No cloud installation
- No endpoint installation (agentless)
- No file server Installation
- No storage platform installation

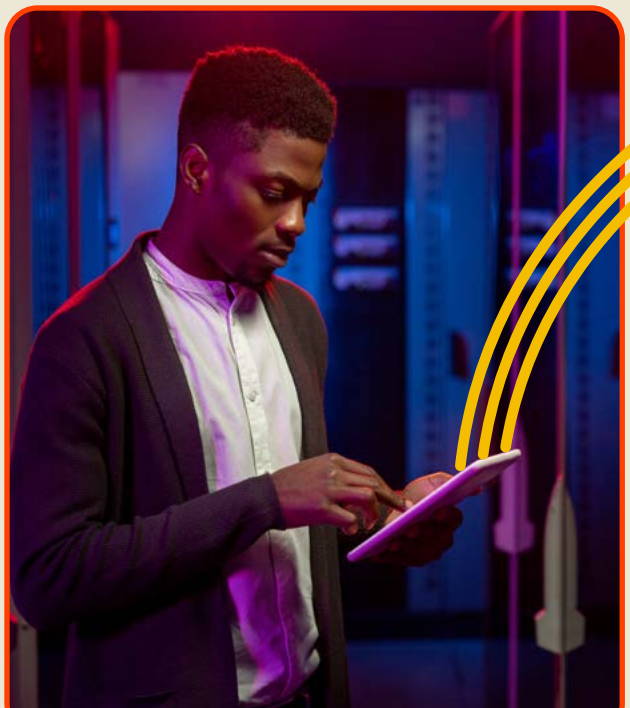
Alerts and integrations

BullWall Ransomware Containment built-in alerting services

- Email notifications
- WhatsApp notifications
- SMS alerts

2-Way interface to RESTful API (pre-configured scripts)

- Splunk
- Cisco ISE
- Windows Defender
- Aruba
- IBM Radar
- McAfee
- Symantec
- TrendMicro
- ForeScout



BullWall Server Intrusion Protection

BullWall Server Intrusion Protection functions as an optional add-on to Ransomware Containment, providing a robust defence against ransomware attacks originating from compromised Remote Desktop Protocol (RDP) sessions. This system will detect unauthorized RDP sessions, alert you, and block the compromised users and servers. It achieves this by implementing a multifaceted approach:

- **Contains intrusion**
  By preventing unauthorized access, BullWall Server Intrusion Protection establishes a containment strategy that effectively prevents ransomware deployment, data encryption, and data exfiltration.

- **Halts breach progression**
  The solution impedes reconnaissance and lateral movement, effectively stopping the potential compromise in other network areas.

- **Defends against compromised credentials**
  Server Intrusion Protection includes an MFA challenge, significantly reducing the threat of unauthorized access, even in the case of stolen credentials. This multi-layered approach ensures a robust defence against RDP-based attacks, making it a vital component in safeguarding organizations against ransomware threats and bolstering their overall cybersecurity posture.

BullWall Server Intrusion Protection includes:

✓ **MFA for RDP sessions |** Easy to use, easy to configure MFA with no requirement for a second device.

✓ **Monitoring of scheduled tasks** | Prevents malware from being installed.

✓ **Immutable record of server access** | Full forensics on all successful and unsuccessful server login attempts.

BULLWALL

Let Ricoh help you enhance your organization's cybersecurity infrastructure. Click here to learn more.

RICOH
imagine. change.