BULLWALL

CIS18 QUICK REFERENCE GUIDE

BullWall is a cybersecurity company that specializes in **automated containment of ransomware and other advanced threats,** primarily through its solution called **BullWall Ransomware Containment.** While BullWall is not a full compliance platform, it can significantly help organizations align with certain controls in the **CIS Controls v8 (CIS18)** framework by **bolstering ransomware containment, detection, and response** capabilities.

Here's how BullWall supports key elements of the CIS18 controls:

CIS SAFEGUARDS BULLWALL CAN HELP WITH

Control 10: Malware Defenses

- **10.1 – Deploy and maintain anti-malware software**

  BullWall complements traditional anti-malware by detecting ransomware encryption activity in real time and automatically stopping it, even if the malware evades AV/EDR.

- **10.4 – Disable or block malicious scripts or code execution**

  By monitoring file shares and data activity, BullWall can detect when malicious encryption begins — regardless of how it was initiated — and stop the offending user/session.

Control 13: Data Protection

- **13.1 – Data Classification**

  Not BullWall's core function, but it helps protect classified or sensitive data from ransomware encryption.

- **13.6 – Securely Dispose of Data**

  While not directly involved in data disposal, BullWall helps ensure data isn't encrypted or stolen prior to secure deletion.

Control 17: Incident Response Management

- **17.3 – Designate Management Personnel to Support Incident Handling**

  BullWall integrates with SIEM/SOAR platforms, providing detailed alerts and logs to support IR teams.

- **17.4 – Conduct Incident Response Exercises**

  BullWall Ransomware Containment can simulate attacks and be used in tabletop or red team exercises to validate response capabilities.

- **17.5 – Conduct Post-Incident Reviews**

  BullWall provides forensics and event data useful for post-mortem analysis after a ransomware event.

Control 16: Application Software Security

Not directly applicable to BullWall's feature set, but by preventing encryption of data by unauthorized or compromised apps, it acts as a containment layer for vulnerable software systems.

Control 18: Penetration Testing

Not directly applicable to BullWall's feature set, but by preventing encryption of data by unauthorized or compromised apps, it acts as a containment layer for vulnerable software systems.

Additional Benefits Relevant to CIS18 Compliance

- **Reduces response time from hours to seconds** by automatically isolating the infected device.
- **Non-signature based —** detects behavior, which helps against zero-day ransomware.
- **Supports regulatory compliance** (GDPR, HIPAA, etc.) by minimizing data loss and breach impact.

SUMMARY MAPPING TABLE

CIS Control	How BullWall Helps
10 – Malware Defenses	Detects and contains ransomware activity automatically
13 – Data Protection	Prevents unauthorized encryption of sensitive files
17 – Incident Response	Provides forensic logs and automated containment
18 – Pen Testing	Supports detection validation in simulated ransomware events

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