RANSOMWARE DEFENSE

Why your backups are only 50% of the solution.

Page 1: The New Ransomware

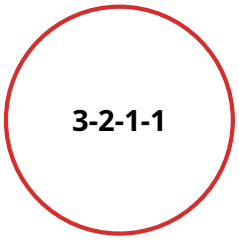
Headline: They don't just lock your data. They steal it.

CardinalsByte Insight: We are now in the era of "Double Extortion." Even if you have perfect backups and can restore your files, hackers will threaten to leak sensitive client tax returns on the dark web unless you pay the ransom.

The Defense: Beyond Backups

To truly protect your firm, you need **Exfiltration Monitoring**. You must detect when massive amounts of sensitive data are being moved out of your network before the encryption process even begins. Reactive protection is no longer enough.

Page 2: The 3-2-1-1 Strategy



3 Copies of your data

2 Different media (e.g., Disk + Cloud)

1 Copy stored strictly offsite

1 Immutable copy (cannot be deleted or altered)

The First 60 Minutes of an Attack

If you suspect a breach, every second counts. Follow this protocol:

1. **Isolate:** Physically unplug infected machines from the network and turn off Wi-Fi to stop the spread.

2. **Do NOT Pay:** Paying does not guarantee data return; it only signals that you are a ”profitable” target for future hits.

3. **Call Your IR Team:** Contact CardinalsByte or your designated incident response team immediately.

4. **Document:** Preserve all system logs and take photos of ransom notes for insurance and FBI reports.