Top 10 Reasons Malware ≠ Ransomware

Stop Confusing the Two: Many IT teams often lump ransomware into the "malware" bucket. That mistake is costly.

Malware makes you sick. Ransomware is terminal.

Only Elastio detects ransomware. We go beyond signatures and alerts to spot encryption at scale, integrity drift, and backup sabotage. While immutability may fix this, pinpointing your last clean recovery point with proof is critical – and only Elastio detects ransomware encryption reliably.

Alerts don't save you. Controlling your recovery does. With Elastio, you don't just detect problems. You control your recovery.

1. All ransomware is malware. Not all malware is ransomware.
Just like all bourbon is whiskey but not all whiskey is bourbon, ransomware is a distinct class of malware. Treating them as the same blinds you how ransomware *really works*.

2. Malware detection ≠ Ransomware recovery.
Malware tools surface known signatures or binaries. Ransomware's impact is behavioral: mass encryption, abnormal I/O bursts, shadow encryption, etc. **Malware** detection says "a bad file is here." **Ransomware** resilience says "your data is encrypted, here's your last clean recovery point and we can prove it."

3. Detection is reactive. Recovery is proactive.
Many signature scans, such as backup malware scans, only ***alert*** you to known threats. Ransomware resilience validates that your recovery points are intact, usable, and provably clean.

4. EDR is for endpoints. Elastio watches data.
EDR tools chase attacker behavior: process spawning, lateral movement, C2 traffic. Elastio analyzes the data itself: encryption drift, KMS anomalies, snapshot deletion. One chases actors; the other protects outcomes.

5. Bad actors prey on the false sense of security.
Traditional malware scans give a false sense of security — a backup can look "clean" while being silently encrypted or corrupted. Without deeper validation, organizations risk catastrophic data loss and prolonged downtime when they actually need to recover.

6. Backups are the new bullseye.
96% of ransomware now target backups. Once compromised, your "last line of defense" disappears. Malware scans don't test backup immutability or restorability.

7. Malware alerts ≠ business assurance.
Your CEO doesn't care about alerts. They care about the business, recovery time, clean data, and reputation. Malware detection does not validate RTO/RPO objectives.

8. Fileless ransomware fly under the radar.
Attackers use legitimate admin tools and in-memory payloads. No malware signature means no detection. But encryption behavior and integrity drift cannot hide.

9. Compliance demands provable recovery.
Regulators (NYDFS, NIST, FFIEC), the board, and insurers require organizations to demonstrate clean, restorable backups. Malware scanning alone won't meet that bar.

10. Alerts don't equal confidence. Assurance does.
Malware detection is table stakes. Provable recovery means clean, tested, immutable backups—and the ability to bounce back without blinking.

Control your recovery >> elastio.com