COVENANT AEGIS REVIEW OF CYBERSECURITY VOL. 6 · NO. 1 · 2026 · PP. 7–26

Anti-Ransomware: Detection, Containment and Resilient Recovery

N. Haddad[1], C. Mwangi[2], A. Petrov[1], S. Okafor[3]

[1]*Covenant Aegis Cybersecurity Division, Threat Research Laboratory*

[2]*Department of Computer Security, Partner Research Network*

[3]*Center for Digital Forensics and Incident Response*

Received 12 Jan 2026 · Revised 1 Mar 2026 · Accepted 7 Mar 2026 · REVIEW ARTICLE · DOI 10.48-CA/cyber.2026.0601 ·
Corresponding author: n.haddad@covenantaegis.com

ABSTRACT

Background. Ransomware combines cryptographic denial of access with extortion and has industrialised through affiliate "ransomware-as-a-service," broadening targets to hospitals and critical infrastructure. **Objective.** To review the technical anatomy of ransomware and the layered defensive strategy—prevention, behavioural detection, containment and resilient recovery—that limits impact. **Methods.** Narrative review of behavioural-detection research (UNVEIL, CryptoDrop) and authoritative guidance (CISA, NIST, ENISA). **Results.** Behavioural signals—rapid high-entropy writes, mass modification, canary-file access—enable early termination where signatures fail; the decisive control against extortion is tested, isolated, immutable backups. **Conclusion.** Durable anti-ransomware combines behavioural early detection, rapid containment and, above all, tested recoverable backups; preparedness and resilience defeat extortion, not payment.

Keywords: ransomware; behavioural detection; extortion; backups; incident response; endpoint security; resilience

1. Introduction

Ransomware encrypts victims' data and demands payment for restoration, increasingly coupled with theft and threatened publication ("double extortion"). Its industrialisation has lowered the barrier to entry and broadened targeting from individuals to hospitals, municipalities and critical infrastructure [1].

2. Anatomy of an Attack

A typical intrusion proceeds through initial access (phishing, exposed services, stolen credentials), privilege escalation and lateral movement, defense evasion and backup deletion, data exfiltration, and finally mass encryption. Modern campaigns dwell in networks before detonation, making early-stage detection more valuable than payload signatures [1,2] (Figure 1).

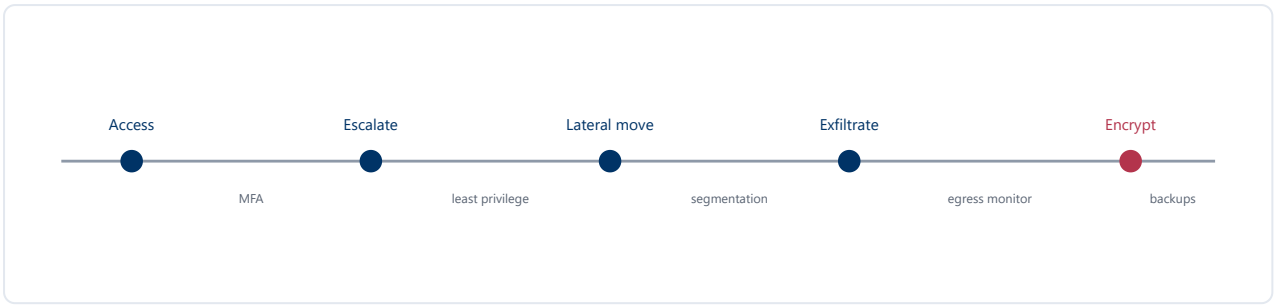


Figure 1. Ransomware kill chain and the defensive control best suited to each stage. Early-stage controls (left) prevent detonation; recoverable backups (right) defeat the extortion even after encryption [1,2]. Schematic.

3. Detection

3.1 Behavioural Approaches

Because payloads are polymorphic, behaviour is a more durable signal than static signatures. UNVEIL detects ransomware by observing characteristic filesystem and desktop behaviours in an instrumented environment [3]. CryptoDrop and related monitors flag the telltale combination of rapid file access, high-entropy writes and bulk modification indicative of encryption, enabling early termination [4]. Decoy or canary files provide a low-false-positive tripwire.

3.2 Limits

Detection must contend with attackers who throttle activity, abuse legitimate tools and disable defenses. No single sensor suffices; correlated endpoint, identity and network telemetry is required.

4. Containment

On detection, rapid isolation of affected hosts, revocation of compromised credentials and segmentation limit spread. Least-privilege access, network segmentation and application allow-listing reduce the blast radius before any incident occurs [5].

5. Resilient Recovery

The decisive control against extortion is the ability to restore without paying. This requires backups that are regular, versioned, tested and isolated—ideally immutable and offline (the 3-2-1 principle and beyond)—so they cannot be encrypted or deleted by the attacker. Authoritative guidance consistently centres recoverable backups, segmentation, MFA and rapid patching as the highest-value defenses [5,6] (Table 1).

Table 1. High-value anti-ransomware controls and the stage they disrupt.

Control	Disrupts	Priority
Offline/immutable backups	Extortion leverage	Critical
MFA everywhere	Initial access	Critical
Segmentation	Lateral movement	High
Behavioural EDR	Encryption stage	High
Rapid patching	Exploited services	High

6. Policy and the Payment Dilemma

Paying ransoms funds the ecosystem, offers no guarantee of recovery and may

carry legal exposure; agencies therefore discourage payment and emphasise preparedness [6]. Effective programs rehearse incident response so recovery decisions are made under plan, not panic.

7. The Covenant Aegis Methodology

Our methodology layers hardening and least privilege, behavioural endpoint detection with canary tripwires, automated isolation playbooks, and immutable, regularly restore-tested backups, validated through tabletop and live recovery exercises. Resilience—measured by recovery time (RTO) and recovery point (RPO)—is the primary metric.

8. Discussion and Conclusion

No prevention is perfect; the residual-risk question is how quickly an organisation can restore. Tables and figures here are illustrative of consensus guidance rather than measured efficacy. Durable anti-ransomware combines behavioural early detection, rapid containment and, above all, tested recoverable backups. Preparedness and resilience—not payment—defeat extortion.

References

1. ENISA. Threat Landscape for Ransomware Attacks. European Union Agency for Cybersecurity; 2022.
2. Kharraz A, et al. Cutting the Gordian knot: a look under the hood of ransomware attacks. *DIMVA*. 2015:3–24.
3. Kharraz A, et al. UNVEIL: a large-scale, automated approach to detecting ransomware. *USENIX Security*. 2016:757–772.
4. Scaife N, Carter H, Traynor P, Butler KRB. CryptoLock (and drop it): stopping ransomware attacks on user data. *IEEE ICDCS*. 2016:303–312.
5. Cybersecurity and Infrastructure Security Agency (CISA). #StopRansomware Guide. 2023.
6. National Institute of Standards and Technology. Ransomware Risk Management: A Cybersecurity Framework Profile (NISTIR 8374). 2022.

9. Threat Evolution and Economics

Ransomware has evolved from opportunistic single-host encryption to organised, affiliate-based "ransomware-as-a-service" (RaaS) operations with double and triple extortion (encryption, data-leak threats and DDoS) [A1]. The criminal economy includes initial-access brokers, negotiators and bulletproof hosting, lowering the barrier to entry. Targeting has shifted toward high-leverage victims—hospitals, municipalities and critical infrastructure—where downtime pressure increases willingness to pay. Understanding this economy clarifies why disruption of leverage (recoverable backups) is more durable than payload-level defenses.

Table A1. Extortion model evolution.

Generation	Leverage	Countermeasure
Single	Encryption	Backups
Double	+ Data leak	Encryption, DLP
Triple	+ DDoS / contacts	Resilience, comms plan

10. Detection Internals

Behavioural detection exploits invariants of bulk encryption: a process rapidly reading many files and writing high-entropy output, often deleting shadow copies and

originals. CryptoDrop monitors file-type changes, similarity (e.g., via similarity-preserving hashing) and Shannon entropy of writes to flag encryption early [A2]; UNVEIL constructs an artificial user environment and watches for tell-tale desktop and filesystem behaviour [A3]. Entropy is a powerful signal because encrypted and compressed data approach maximal entropy, distinguishing them from typical documents. Figure A1 illustrates the entropy separation underpinning detection.

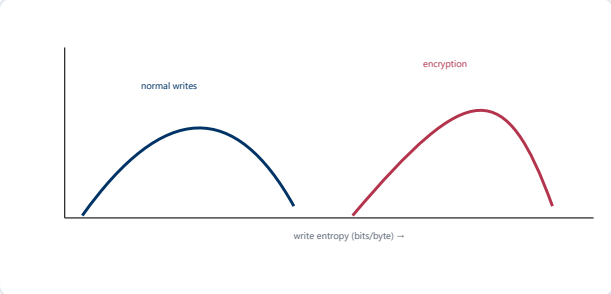


Figure A1. Schematic: encrypting processes produce near-maximal-entropy writes, separable from typical document writes—the basis of entropy-based ransomware detection [A2]. Conceptual.

11. Cryptographic Reality and Decryption

Modern ransomware uses sound hybrid cryptography (symmetric file keys protected by asymmetric keys held by the attacker), so decryption without the key is generally infeasible. Recovery therefore depends on implementation mistakes (occasionally yielding free decryptors via initiatives such as No More Ransom) or, reliably, on backups. This asymmetry is why authoritative guidance centres preparedness over hope of cryptographic recovery [A4].

12. Backup Architecture and Recovery Objectives

Recoverability is engineered through the 3-2-1(-1-0) principle: multiple copies, on different media, with an offsite and an offline/immutable copy, and verified (zero-error) restores. Immutability (WORM storage or object-lock) prevents attackers with domain privileges from deleting backups—an explicit step in modern intrusions. Recovery objectives (RPO, RTO) must be defined per system and validated by live restore tests, because untested backups frequently fail when needed [A4,A5].

13. Governance, Exercises and the Payment Question

Authoritative guidance (CISA, NIST, ENISA) discourages paying ransoms: payment funds the ecosystem, does not guarantee recovery and may carry sanctions exposure [A4,A6]. Mature programs codify incident-response playbooks, conduct tabletop and live recovery exercises, and pre-decide escalation and communication so that decisions under attack follow a plan. Cyber-insurance and legal/regulatory reporting obligations are integrated into the plan.

14. Sector Considerations: Healthcare and OT

Healthcare and operational-technology environments face elevated stakes: encryption can disrupt patient care or physical processes, and legacy/embedded systems resist standard endpoint controls. Defenses emphasise segmentation between IT and clinical/OT networks, manual fallback procedures, and tested continuity plans so that essential services persist through an incident.

15. Future Directions

Priorities include earlier, lower-false-positive behavioural detection, hardware-assisted and immutable backup by default, automated isolation and recovery orchestration, and resilience metrics (verified RTO/RPO) as primary KPIs. The enduring principle is that preparedness and tested recovery—not payment—defeat extortion.

Extended References

7. ENISA. Threat Landscape for Ransomware Attacks. 2022.
8. Scaife N, et al. CryptoLock (and drop it): stopping ransomware attacks on user data. *IEEE ICDCS*. 2016:303–312.
9. Kharraz A, et al. UNVEIL: a large-scale, automated approach to detecting ransomware. *USENIX Security*. 2016:757–772.
10. CISA. #StopRansomware Guide. 2023.
11. NIST. Ransomware Risk Management: A Cybersecurity Framework Profile (NISTIR 8374). 2022.
12. FBI / CISA joint advisories on ransomware (discouraging payment). 2021–2023.

Author contributions: NH led the review; CM and AP analysed detection/containment; SO contributed forensics and recovery. All authors revised. **Funding:** Covenant Aegis Cybersecurity Division. **Competing interests:** Authors are affiliated with Covenant Aegis.

© 2026 Covenant Aegis Cybersecurity Division. This review synthesises publicly available peer-reviewed literature and authoritative defensive guidance (CISA, NIST, ENISA); figures are illustrative. For professional and educational use.