Data Sheet

Taming Cyber Insurance Costs Against Ransomware Volatility

Ransomware is the dominant driver of cyber insurance costs, and most security investments do almost nothing to change that. EDRs, SIEMs, and backup solutions were built for a different threat landscape. Ransomware operators know exactly how those tools work, and they design their attacks around those limitations. The gap between what organizations have deployed and what ransomware actually demands is where claims are born.

Ransomware demands a security control built specifically to stop it. The Halcyon Anti-Ransomware Platform prevents ransomware from executing, stops data exfiltration before it becomes leverage, and recovers encrypted systems without paying a ransom, reducing both the frequency and severity of the claims that drive premiums up.

The Halcyon Difference

Halcyon is purpose-built from the ground up to defeat ransomware.
The Anti-Ransomware Platform takes an end-to-end approach across the full attack lifecycle, from pre-execution through exfiltration and encryption, while the Halcyon Ransomware Operations Center (ROC) provides 24/7/365 expert management included with every deployment at no extra charge.

- **Ransomware Protection:** Halcyon is the only vendor with AI/ML models trained specifically on ransomware to stop even unknown variants from executing, including attacks using BYOVD techniques and living-off-the-land tactics that bypass traditional endpoint tools.
- **File Resilience and Decryption:** File Resilience monitors every file operation from the deepest layer of the operating system, identifying ransomware behavior the moment it begins and reversing attempted changes before encryption can take hold. If encryption ever does succeed, Halcyon can capture encryption key material in real time, enabling decryption and instant recovery without relying on backups.
- **Exfiltration Protection:** Halcyon Data Exfiltration Protection (DXP) identifies signals that data is being staged and exfiltrated before encryption begins, preventing the data theft that drives double extortion demands.
- **Ransomware Operations Center:** The ROC is staffed exclusively by ransomware specialists in TTPs, cryptography, threat intelligence, malware reverse engineering, and incident response. Their sole focus is detecting the activity that precedes

COSTS OF AN INCIDENT

$5,080,000

Average total cost per ransomware or extortion incidents in 2025, including investigation, downtime, legal exposure, and reputational damage. (IBM Cost of Data Breach Report 2025)

$1,530,000

Average recovery cost in 2025, excluding any ransom payment. The gap between recovery cost and total incident cost reflects downtime, IR, and legal exposure. (Sophos State of Ransomware 2025)

encryption: credential abuse, lateral movement, reconnaissance, and the misuse of trusted tools. These signals are easy to miss when you are monitoring for everything. They are nearly impossible to miss when ransomware is all you do.

Building Ransomware Resilience Insurers Recognize

Ransomware risk is now a line item in every underwriting conversation. Insurers assess the likelihood and potential severity of a claim when underwriting a policy, and organizations that can demonstrate meaningful ransomware controls are better positioned to negotiate favorable terms, whether that means improved sub-limits, lower deductibles, or greater pricing stability at renewal.

The Halcyon Anti-Ransomware Platform reduces the conditions that lead to claims in the first place: preventing encryption, stopping data exfiltration, and shortening response timelines from weeks to hours. That translates directly to a lower probability of a covered loss, which is the foundation of any productive conversation with an insurer. While premium outcomes will always depend on the specific insurer, policy structure, and broader market conditions, demonstrating provably effective ransomware controls gives your security and finance teams a substantive and credible case to make at the negotiating table.

The Benefits for Your Business

Halcyon's ability to prevent ransomware from executing, capture encryption keys for automated recovery, and stop sensitive data loss before it becomes leverage delivers measurable outcomes across operational, financial, and compliance dimensions:

- Reduce the risk of ransomware-driven downtime and business disruption
- Recover from an incident in hours rather than days or weeks
- Prevent sensitive data loss and the extortion demands that follow
- Maintain compliance and reduce exposure to lawsuits and regulatory action
- Protect brand reputation with customers and partners
- Strengthen your position negotiating cyber insurance with demonstrated ransomware efficacy, supporting a case for higher sub-limits, lower deductibles, and reduced co-insurance
- Add 24/7 ransomware expertise through the ROC without adding headcount

Global 2000 companies rely on Halcyon to defeat ransomware with minimal business disruption through purpose-built bypass and evasion protection, file resilience, key material capture and decryption, and exfiltration and extortion prevention.

Ready to see how Halcyon performs against your threat environment? Request a demo by emailing us at info@cyberfortgroup.com.

BREACHES & INCIDENTS

44%

of all confirmed breaches now involve ransomware, up 37% year over year. (Verizon 2025 DBIR – verizon.com/business/resources/reports/dbir)

7,515

organizations appeared on dark web leak sites in 2025, a 58% year-over-year increase and the highest annual total ever recorded. (GuidePoint Security GRIT 2026 Annual Report)

THE SEVERITY OF CLAIMS

$1,000,000

Median ransom payment in 2025, down 50% year over year, yet 52% of all payments still exceeded $1M and 57% of demands were $1M or higher. (Sophos State of Ransomware 2025)

$75,000,000

Largest confirmed ransomware payment on record, made by an unnamed Fortune 50 company in 2024, a single claim that would exceed most policy sub-limits. (Record-Breaking $75M Ransomware Payment, PC MAG)