halcyon

Taming Ransomware Cost Volatility for Cyber Insurers

Halcyon is the only anti-ransomware platform that prevents business downtime and stops data extortion attacks. Our flagship Halcyon product combines ransomware prevention, encryption key capture, automatic file decryption, and data exfiltration protection (DXP) into a single product. Backed by a ransomware warranty, Halcyon reduces the time spent recovering from a ransomware attack from days and weeks down to minutes and hours.

OUR APPROACH TO STOPPING RANSOMWARE

With a large amount of ransomware claims paid out, and rising premiums for policy holders, something must be down to lower the risk level and slow down the success of cybercrime groups. Halcyon has developed a unique approach that goes beyond traditional endpoint security controls and backup solutions to target the core problem of ransomware directly.

Prevent Ransomware: We are the only vendor with AI/ML models trained entirely on ransomware TTPs to stop even unknown variants from running.

Intercept the Keys: We capture and intercept the encryption process that occurs during ransomware execution, preventing the need to pay any ransom ever.

Stop Data Leaks: Our DXP engine automatically prevents mass data movement triggered by a ransomware campaign across the entire organization.

THE RESULTS:

- **ZERO ransoms paid by 200+ enterprise clients.**
- **ZERO Halcyon customers listed on data leak sites.**
- **ZERO bypasses or evasions of our agent vs. 2,650 EDR bypasses recorded by Halcyon customers.**

RECALIBRATING RANSOMWARE RISK CONTROLS VALUE

Ransomware is not a new threat, but the industry has been slow to recalibrate risk and the types of controls needed to adequately scope the true impact of this threat. Considering ransomware can create $1B USD damages as in the case of United Health in 2024 or have ripple effects that lead to statewide emergency declarations as in the case of Colonial Pipeline in 2021, both new risk calculations and proactive next-generation security controls are needed to respond appropriately.

RANSOMWARE COSTS

- Up to 60% of costs are owing to extortion, while incident response account for up to 40%.
- The average victim downtime is 22 days.
- Ransomware IR costs for a large enterprise average $5.1M per incident.

BREACHES & INCIDENTS

- Over one-third of all attacks involved ransomware.
- 51% of attacks now appear to use double extortion - where threat actors encrypt AND exfiltrate data to extort you.
- 95% Growth YoY – more than 4,300 reported incidents in the USA in 2023 and only ~20% are reported!

CLAIMS SEVERITY

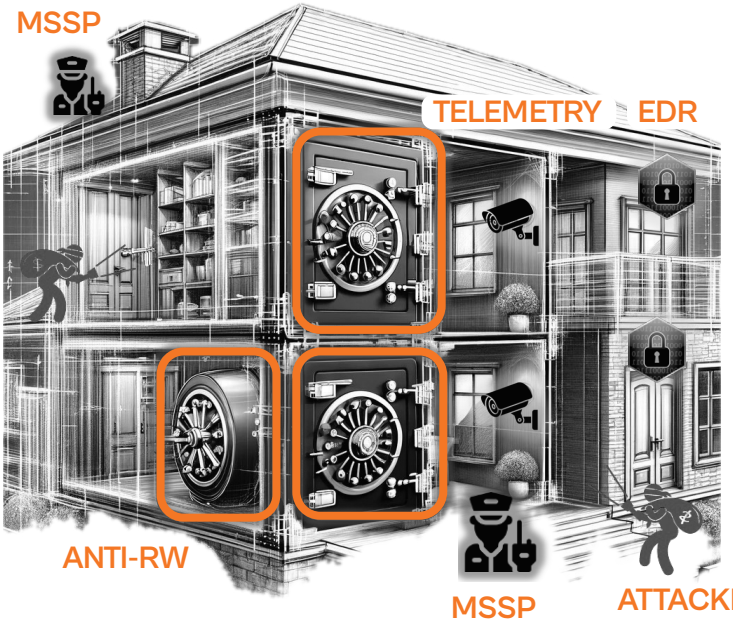
- Ransomware is the most common cyber insurance claim type, averaging ~29%.
- Cost of claim is 300% higher when DFIR recovery is initiated.
- From 2022 – 2023 claim severity rose 117%.
- Average increase in ransom demand to $1,600,000 USD.

While many products, tools and solutions exist to combat the wide variety of cyberattacks, none aside from Halcyon focus entirely on eliminating business downtime and damages from ransomware attacks. Most traditional controls are scoped to a specific threat type i.e. phishing, anti-malware or malicious insider threats but ransomware groups chain multiple methods, leverage a variety of techniques and can quickly change tactics on the fly.

RECALIBRATING RANSOMWARE RISK CONTROL VALUE

We propose a new model of risk based on the control efficacy and how it positively or negatively impacts the claim costs for a ransomware incident. By scoping a risk control to the actual reduction in cost of a payout and the damage that can be done to a victim organization, we can show return-on-investment for implementing new controls.

In this example, we map cyber risk controls to that of physical security to understand the framework of cyber breaches more easily:



Risk Control	Property Analogy	Value (Control Efficacy, Claim Cost)
Anti-Ransomware	Whole House Strongbox	High
EDR	Locks, Alarms	Medium
Data Exfil Prevention	Strongbox	High
Telemetry	CCTV	Low
MS/SP	Sec Monitoring + Response	High

THE OUTCOMES

Halcyon's unique ability to prevent ransomware from running, capture encryption keys, stop data leaks, and assist in automated data recovery provides several positive outcomes to businesses of all sizes.

- **Never pay a ransom for your data again**
- **Eliminate business downtime and recover from a ransomware incident in hours vs. days and weeks.**
- **Protect your brand's reputation with consumers.**
- **Reduce claims payouts for ransomware incidents.**
- **Maintain compliance with data privacy laws and reduce potential lawsuits and regulatory actions.**

Security controls have a bad reputation for increasing friction and getting in the way of productivity, that is until an incident occurs that impacts the revenue generating parts of the organization. For security to be considered indispensable and not simply an item on a budget sheet, it needs to demonstrate a true reduction in material risk to the business while being simple and invisible to employees. **To learn more about Halcyon visit** halcyon.ai