

# Technology Overview: Making Ransomware History

## The Ransomware Threat

According to the most recent estimates, as many as 50% of organizations have experienced a ransomware attack in the last two years. Ransomware is no longer considered just a technical threat, but rather the largest single risk to any organization.

In 2021 the impact from ransomware attacks is estimated at \$20 billion dollars in the US alone. Data exfiltration and the threat of exposure are now commonly part of more complex ransomware operations, or *RansomOps*, and work to compound the overall impact to victim organizations and increase the chances of success for the extortionists.

Current solutions available in the market, while robust and effective for some threats, do not fully protect against ransomware attacks because they were tooled to find malware variants in general, but were simply not designed to recognize ransomware. Furthermore, ransomware operators are implementing novel advanced evasion techniques into their payloads specifically designed to evade or completely circumvent traditional endpoint protection solutions.

## The Halcyon Advantage

### RANSOMWARE SPECIFIC AI/ML MODELS

Halcyon incorporates an industry-first capsule-network-based machine learning approach to AI implementation with the following key features:

- **Collaborative decision-making in which each micro-model communicates with the others, and provides weighted decisions to facilitate collaborative decisions on actions as a group.**
- **The ability to be trained, learn, and make highly accurate decisions with fewer data input than traditional convolutional neural network models.**

### API-DRIVEN

Halcyon was built with a modern SOC in mind. Modern security infrastructure deploys multiple solutions managed through multiple consoles, which means more complexity in the SOC. Halcyon not only provides a SaaS web interface model, but we also designed our platform to integrate as much as possible with your existing security stack.

### HALCYON FEATURES:

- Four layers of ransomware prevention and protection:
  - Pre-Execution
  - Exploitation
  - Behavioral
  - Resiliency
- Exceptionally low system resource consumption
- Supports Windows 10 & 11, Windows Server: 2012 R2, 2016, 2019, 2022
- Simple deployment with no reboots required

### THE HALCYON STORY

Based in Austin, TX, Halcyon was founded in 2021 by a team of cyber industry veterans after battling the scourge of ransomware and advanced threats for over a decade at some of the most innovative and disruptive security vendors of our day, including leaders from Cylance (now Blackberry), Accuvant (now Optiv), and ISS X-Force (now IBM). Halcyon is focused on building products and solutions for mid-market and enterprise customers that give organizations the edge against ransomware and other advanced threats.

## MULTI-LAYERED DETECTION AND PREVENTION

Halcyon is designed to measure a process over time in diverse ways to help drive accurate decisions. Every analysis layer flows data into a multitude of decision engines for untrusted/unknown processes:

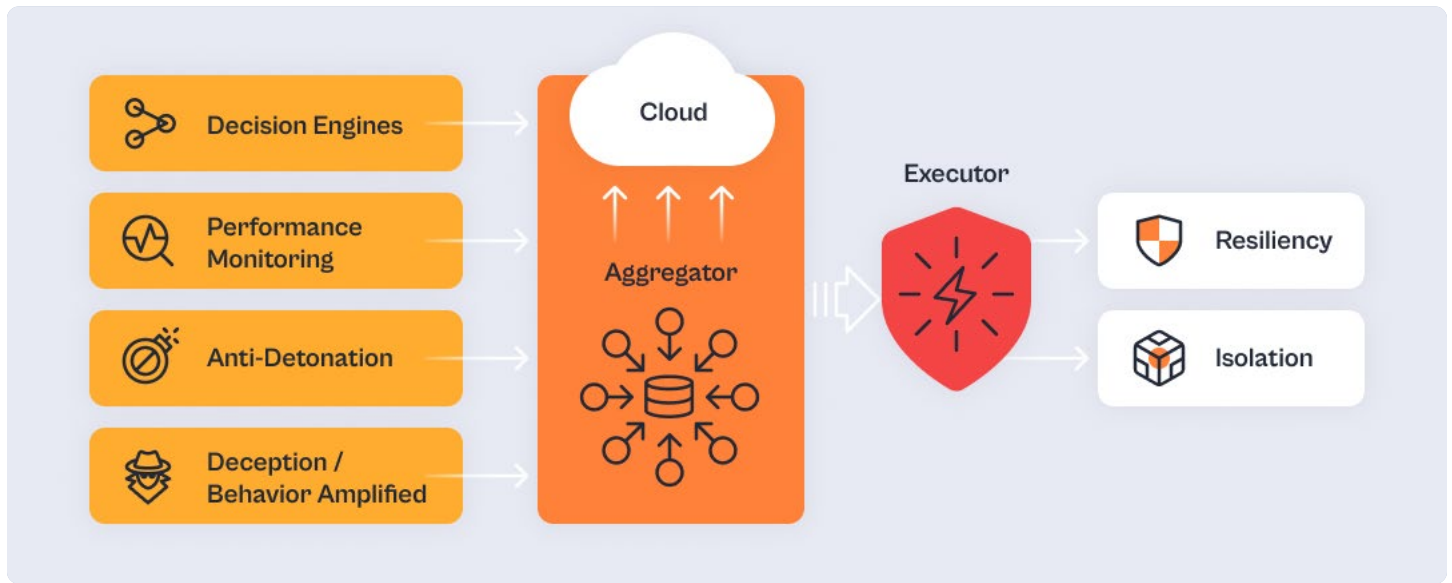


Figure 1: Pre-Execution >>> Exploitation >>> Behavioral >>> Resiliency

## The Halcyon Anti-Ransomware and Cyber Resilience Platform

Halcyon's unique anti-ransomware platform is easy to deploy, does not conflict with existing endpoint security solutions, and provides several unique levels of protection against ransomware attacks. Halcyon is the first platform to leverage AI/ML to specifically target the problem of ransomware.

For more information on how Halcyon efficiently and effectively defeats ransomware attacks, contact our Sales Team at [sales@halcyon.ai](mailto:sales@halcyon.ai) or visit [halcyon.ai](https://halcyon.ai) to request a free ransomware readiness report today!

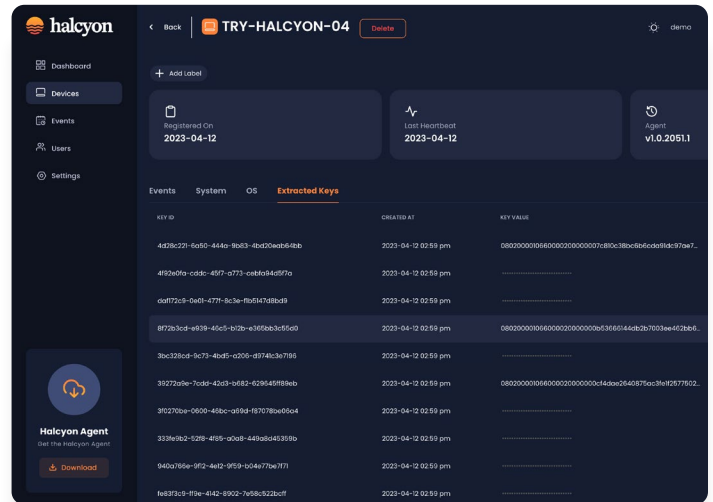


Fig 2: Halcyon Platform - Extracted Keys from Devices