halcyon

Better Together: The Halcyon Partner Program

About Halcyon

A team of cybersecurity veterans founded Halcyon after witnessing ransomware disrupt organizations and the lives of millions unabated for a decade. Existing anti-malware solutions claim to be effective against ransomware attacks, but the evidence has proved otherwise, which begs the question... why?

How Ransomware Is Different

Ransomware is fundamentally different from other forms of malware as it is, by nature, disruptive to an organization. Remote Access Trojans provide ingress into networks and info stealers exfiltrate sensitive data, but neither grind business operations to a halt. Moreover, the rise of Ransomware as a Service (RaaS) gangs mimic the more conventional Software as a Service business model in every meaningful measure. These groups generate income that any legitimate software vendor would envy, and this provides a profit motive that drives innovation.

We see this most clearly in the evolution of the extortion tactics employed by the ransomware actors. Originally, the malicious payloads would encrypt files and demand payment for decryption keys. Security teams found success in either restoring from backups or accepting the loss of data as an acceptable consequence. Cybercriminals evolved and built data exfiltration capabilities into their malware, which gave rise to Double Extortion schemes: attackers not only demand payment of a ransom to regain access to encrypted systems, but they also further threaten to expose an organization's sensitive data publicly or sell it to competing interests.

More recently, ransomware actors have employed Triple and Quadruple Extortion schemes, which include employing denial of service (DoS) attacks and harassing of clients, vendors or partners until the victim pays.

The Cost Of Ransomware

This translates to massive costs for victims. The costs following a ransomware attack average more than $2M per incident per target organization, and this figure does not include costs like damage to the brand, lost revenue and production from system downtime, or other collateral damage. The impact of these numbers is staggering, especially if we compound those costs against the United States Department of Justice estimate that more than 4,000 ransomware attacks are undertaken daily.

Partnering With Halcyon

Traditional security solutions claim to be effective in detecting and preventing ransomware, but the evidence tells a different story. Colonial Pipeline and other attacks demonstrate that these solutions can be easily circumvented. Halcyon designed our platform to deal with the specific TTPs that ransomware actors leverage.

Halcyon: The Force Multiplier

The *Halcyon Anti-Ransomware and Cyber Resilience Platform* is not designed to replace or interfere with existing security tool deployments, but instead delivers capabilities that work to enhance the efficacy of these solutions as well as provide protection against advanced and novel ransomware variants. In fact, our solution can amplify signals generated by ransomware to better help existing security products trigger earlier for malicious events.

API-DRIVEN TO EASILY INTEGRATE WITH YOUR TECHNOLOGY STACK

We understand consoles have a place in the modern security stack, but we built our platform with an API-first mentality. This means you can access anything related to Halcyon programatically. Want to power your security program with Halcyon's leading technology? We have you covered natively.

LIGHTWEIGHT AND CONFLICT FREE

Our platform utilizes an agent with a remarkably small footprint on host systems because we are focused solely on detecting and preventing ransomware. Moreover, we test extensively in conjunction with other solutions such as Microsoft Defender and Crowdstrike Falcon so that your security team can focus on fighting ransomware infections instead of remediating configuration conflicts between your security solutions.

THE HALCYON DIFFERENCE

Endpoint security products are built to cover a lot of ground in defending against malware of all types. The Halcyon Platform is purpose-built to defeat ransomware with multiple layers of defense that deliver efficient endpoint resilience.

PRE-EXECUTION PREVENTION

Halcyon leverages multiple AI/ML conviction models that defend against ransomware pre-execution. Our advanced AI/ML decisioning models were trained solely on ransomware samples, making them far more efficient and effective than models trained to look for more common forms of malware. Moreover, our agent employs a proprietary kernel architecture, which means that we can provide deeper inspections than almost any other tool on the market.

ANTI-EVASION

We built our solution with an emphasis on the attacker mindset. Our analysis revealed that ransomware often performs multiple checks before executing to avoid analysis or victimizing unintended targets. We exploit these features by aggravating the payload, prompting the ransomware to react defensively to avoid detection, forcing the malicious operation to terminate as a protective measure.

ENDPOINT HARDENING

The Halcyon Platform provides multiple mechanisms that further harden endpoints against ransomware infections. Malicious payloads often attempt to blind or unhook existing endpoint solutions, but Halcyon is designed to detect and prevent attacks that circumvent traditional security tools. In addition, Halcyon amplifies early attack signals to enhance the detection capabilities of existing endpoint solutions to reveal malicious payloads earlier that otherwise would not have been detected.

RANSOMWARE KEY EXTRACTION

We understand that ransomware operators are actively investing in R&D and further evolving their capabilities to remain effective against security solutions, and we acknowledge that no solution on the market is 100 percent effective. We have designed our solution to protect our clients with defense-in-depth failure in mind. On the rare occasion that a ransom payload executes, we can autonomously isolate the impacted device to protect the larger network, neutralize the attack in progress and quickly recover and restore the impacted endpoint.

Partnering with Halcyon

Want to become a partner with Halcyon? Reach out to partners@halcyon.ai or visit our website at halcyon.ai/partners

HALCYON AGENT

Key aspects of the Halcyon Platform advantage include:

- Full API access
- Intuitive web console
- Unattended installs
- No reboot required
- Exceptionally low impact on system resources

SUPPORTED SYSTEMS

These following systems are currently supported by Halcyon:

- Windows 10 & 11
- Windows Server 2012 R2, 2016, 2019, 2022

FUTURE SUPPORT

These following are slated to be covered by Halcyon soon:

- Linux
- MacOS