

Executive Overview of Halcyon Keyless Decryption

Halcyon Keyless Decryption™

Halcyon has built a new service line dedicated to assisting the victims of ransomware attacks that leverages our patented Keyless Decryption™ capabilities, specifically designed to enable victim organizations to recover impacted systems and data without the need to pay a ransom demand and without getting hit with extensive remediation costs.

Halcyon analysts have identified exploitable weaknesses for many of the top ransomware operations which enable us to reverse the impact of attacks, decrypt impacted systems and data and restore business operations, even if Halcyon was not deployed on the impacted systems prior to the encryption event.

How it Works



Step 1: Viability Assessment

Halcyon provides your organization with a zero-cost consultation to demonstrate proof of value by delivering Keyless Decryption™ examples of your organization's decrypted data based on samples of attacker encrypted files your organization has provided.

This service is available to address ransomware variants for which Halcyon has already developed a decrypter, and the recovery process can commence with formal client engagement. For novel ransomware variants, we request your organization provide a sample of the ransomware payload as well as any available information on the attacker's TTPs and infrastructure telemetry for analysis so a Keyless Decryptor can be developed.



Step 2: Analysis

Halcyon investigates vulnerabilities in the attack and/or payload code base leveraging our extensive understanding of ransomware operations and the latest in cryptology implementations to develop a Keyless Decryptor. We determine if it is possible to recover some or all of the impacted systems and data, and the recovery process can commence with a formal service engagement.

(Continued on next page...)

Halcyon Features

- Three layers of ransomware security capabilities:
 - Pre-Execution Prevention
 - Attacker Behavior Detection
 - Data Decryption and Recovery
- Low system resource consumption
- Simple deployment with no reboots required

The Halcyon Story

Based in Austin, TX, Halcyon was founded in 2021 by a team of cybersecurity 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.



Step 3: Recovery

Once it has been established that Halcyon Keyless Decryption™ capabilities can remediate the impact of the attack, the formal engagement commences with deployment of the Halcyon Anti-Ransomware Platform. Our agent, in addition to its prevention and resilience capabilities, acts as the Keyless Decryption™ tool in your environment.

If for some reason Halcyon cannot serve the client based on the assessment and analysis process, there is absolutely no cost to your organization.

Customer Case Study: Novel Ransomware Attack

On May 20, 2023, a manufacturing company with revenue nearing \$1B annually was successfully attacked, encrypting all Windows workstations and servers while destroying data backups, significantly disrupting business operations, and rendering recovery contingencies all but moot in the process.

At that time, the organization engaged an incident response and data restoration service provider to assist in the recovery. After two days of negotiating, they made the difficult decision to try to rebuild all their systems from scratch. The estimated time for full recovery would be several months given the need to bring in multiple technology partners to assist them in the process.

Following a short assessment period, Halcyon Keyless Decryption™ capabilities quickly recovered their most critical asset, a Cisco Contact Center server which provides telephony services for the company.

This allowed them to restart their call centers and return to taking orders and providing customer care, restoring these critical business operations. Halcyon then proceeded to restore 90% of impacted file shares, 95% of their critical server infrastructure, and most local files that were lost in the attack through our Keyless Decryption™ capabilities.

In short, Halcyon Keyless Decryption™ recovered systems and data within hours of being engaged and returned the business to operational in less than a week at a fraction of the proposed months-long recovery plan.

Halcyon Keyless Decryption™ capabilities will dramatically change the balance of power in the attacker-victim equation and give your organization a better option for ransomware recovery than ever before. For more information about Halcyon Keyless Decryption™ and to request a formal quote, contact services@halcyon.ai or [visit halcyon.ai](https://halcyon.ai) to learn more.

See the Halcyon Difference for Yourself

[Halcyon](#) is the only cybersecurity company that eliminates the business impact of ransomware. Modern enterprises rely on Halcyon to prevent ransomware attacks, eradicating cybercriminals' ability to encrypt systems, steal data, and extort companies. Backed by an industry-leading warranty, the [Halcyon Anti-Ransomware Platform](#) drastically reduces downtime, enabling organizations to quickly and easily recover from attacks without paying ransoms or relying on backups.