halcyon

Data Sheet

Feature Spotlight: File Resilience

Ransomware lost its most powerful weapon.

The Problem

By the Time Traditional Security Acts, Files Are Already Encrypted

Ransomware doesn't wait for your security stack to catch up. Once a payload executes, encryption can begin within seconds, long before most tools have even generated an alert. Most endpoint security tools detect ransomware only after encryption begins, relying on signatures, threat intelligence, or known attack patterns that require a **"Patient Zero"** to identify a new threat. Once files are encrypted, the damage is done: recovery is measured in weeks, not minutes.

What's needed is a fundamentally different approach, one that operates where ransomware can't hide, catches it the moment it acts, and keeps your business running without skipping a beat. Here's how Halcyon File Resilience does exactly that.

How It Works

Ransomware Encrypts Your Files. Halcyon File Resilience Gives Them Back, Instantly.

File Resilience operates at the deepest layer of the operating system, giving Halcyon visibility into file activity that no user-space security tool can match. The moment a process starts behaving like ransomware, File Resilience knows, and so does your team.

- **Always watching.** File Resilience monitors every file operation happening on your endpoint in real time, tracking the exact behavioral patterns ransomware can't avoid exhibiting.
- **Encryption caught instantly.** The moment a process starts encrypting files, File Resilience identifies it, whether it's a known ransomware family or a brand-new variant no one has ever seen before.
- **Full visibility, immediately.** Alerts are routed to Halcyon's ROC and your management console at the same time, so your team and Halcyon's experts are working from the same picture from the first second.
- **Experts evict the threat.** Halcyon's ROC, included 24/7/365, reviews the event and works directly with your team to investigate, contain, and evict the threat actor, before the attack has a chance to go further.

Halcyon Features

- AI & Behavioral Engine
- **File Resilience**
- EDR Tamper Detection
- Bring Your Own Vulnerable Driver (BYOVD) Protection
- Data Exfiltration Protection (DXP)
- Key Material Capture & Decryption
- Ransomware Operations Center

About Halcyon

Halcyon is the only cybersecurity company that eliminates the business impact of ransomware. Unlike tools that detect and respond after damage is done, Halcyon is built to make sure ransomware never succeeds, backed by an industry-leading warranty and a platform purpose-built to stop encryption, exfiltration, and extortion at every stage of an attack. Halcyon Anti-Ransomware Platform drastically reduces downtime, enabling organizations to quickly and easily recover from attacks without paying ransoms or relying on backups.

File Resilience Benefits

See What Others Miss.	Never Face It Alone.	No New Software. No New Work.	Built Into a Platform That Never Stops.
By operating at the kernel level, File Resilience catches encryption activity that evades signature-based, and cloud-dependent tools.	Every detection is backed by Halcyon's ROC, expert analysts available around the clock to investigate, coordinate, and evict threat actors on your behalf.	File Resilience ships as part of the standard Halcyon agent. If you're already a Halcyon customer, it's already working. No installation, no configuration, no hassle.	File Resilience is one layer in Halcyon's defense-in-depth approach. Even when an attack pushes further, the platform has another answer, ensuring your data and your business are protected at every stage.

Behavioral Encryption Detections

- High-entropy write detection
- Known ransomware extension blocking
- File header corruption detection
- Read-Delete-Encrypt-Write pattern detection
- Real-time kernel-level blocking

To learn more about Halcyon File Resilience or any other aspect of the Halcyon Anti-Ransomware Platform, visit halcyon.ai and schedule a personal demo with one of our ransomware experts.

Halcyon Anti-Ransomware Platform

Eliminate ransom payments, ensure operational continuity, and prevent data extortion.

Endpoint Protection Evaded	Halcyon Endpoint Agent	Pre-execution Cloud Detection	Expert-led Threat Response	Ransomware Recovery
• EDRs are disabled or blinded • Evasion of signatures and signals • Missed alerts	• Collects data • Blocks known threats • EDR tamper detection • Sends data to cloud for further analysis	• Detect initial compromise and LOTL techniques • Kill nefarious processes • BYOVD protection • Data Exfiltration Protection (DXP)	• Isolates endpoint(s) • Notifies your team • Blocks C2 communication • Fleet inoculation	• File Resilience • Key Material Capture • Reverse engineering of encryption keys • ROC-led decryption of data

24/7 Halcyon Ransomware Operations Center (ROC) Team