Halcyon Anti-Ransomware Platform Technical Deep Dive

The Halcyon Anti-Ransomware Platform is the first security platform that delivers comprehensive protection against the business impacts of ransomware across all stages of an attack. Backed by a team of ransomware experts monitoring the platform around the clock, Halcyon provides unparalleled protection against damaging ransomware attacks without requiring security teams to replace anything they currently use or add additional staff. Read on to learn how the features and capabilities work before, during, and after an attack to keep your organization secure.

Before Attack

Our Before Attack protection targets preventing any potential ransomware file, executable, or process from executing on a protected endpoint. The prevention AI models are trained on one of the world's largest ransomware repositories. This allows Halcyon to root out ransomware files and processes attempting to circumvent traditional endpoint security product detection. With over 10,000 variants of ransomware prevented to date, Halcyon's before-attack protections have yet to miss any ransomware at any of our fully protected customers.

During Attack

Halcyon During Attack protection employs a proprietary micro-model architecture designed on the principle of capsule network-based machine learning that enables broad benefits over previous behavioral analysis methods, including:

- Data-driven supervised and unsupervised learning engines work together across endpoints and the entire organization to analyze and convict suspicious processes in real-time.

- Efficient analysis by leveraging several AI/ML models in parallel instead of relying on one monolithic detection model that may or may not be effective against a novel ransomware variant.

- Highly accurate conviction with a limited dataset as each micro-model is specialized and assigned behavior sets that feed data into other micro-models to leverage in their decisions.

- Process tracing to detect and combat process injection attacks targeting security products on a system.

Halcyon Features

- Always Included 24/7/365 Expert Threat Monitoring and Recovery

- Pre-execution Prevention

- Ransomware Behavior Detection

- Encryption Key Material Intercept

- Data Exfiltration Prevention

About Halcyon

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.
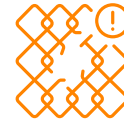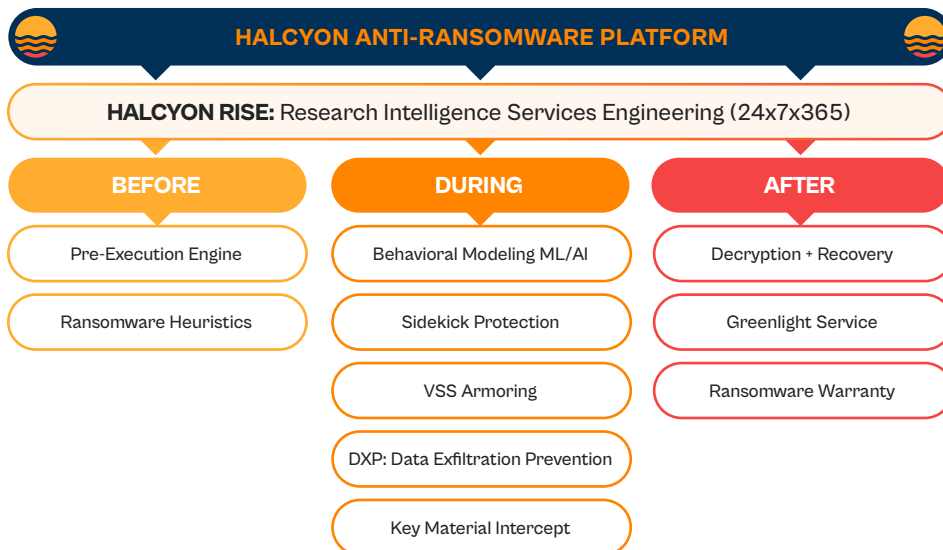
After Attack

Before and During attack protections are backed by several After Attack capabilities designed to prevent a ransomware infection from spreading to other endpoints, reducing the potential impact of a successful attack. Halcyon employs several methods of reducing the effect on an endpoint if a ransomware event occurs, including:

- Ransomware encryption key capture and recovery that triggers any time ransomware-initiated encryption occurs on a system.

- Hardening of Volume Shadow Service (VSS) to ensure that ransomware cannot delete or corrupt critical system backup snapshots.

The During and After Attack protections work in tandem to ensure that if the detection of a malicious process is missed, recursive action is taken to kill the child, and parent process that is performing the malicious activity, such as writing known malicious extensions to files.

The During and After Attack protections work in tandem to ensure that if the detection of a malicious process is missed, recursive action can be taken to kill the process that is performing the malicious activity, such as writing known malicious extensions to files.

HALCYON ANTI-RANSOMWARE PLATFORM

HALCYON RISE: Research Intelligence Services Engineering (24x7x365)

BEFORE	DURING	AFTER
Pre-Execution Engine	Behavioral Modeling ML/AI	Decryption + Recovery
Ransomware Heuristics	Sidekick Protection	Greenlight Service
	VSS Armoring	Ransomware Warranty
	DXP: Data Exfiltration Prevention	
	Key Material Intercept	

Halcyon: First in Defeating Ransomware

Ransomware is one of the biggest threats facing organizations today. Modern endpoint protection products are losing the battle against ransomware, as evidenced by the daily headlines announcing yet another breach. Halcyon is designed to work alongside existing endpoint security products and can be deployed into previously compromised environments to prevent ransomware from executing.

For more information on how Halcyon efficiently and effectively defeats ransomware attacks, **visit halcyon.ai** and **schedule a personal demo** today!