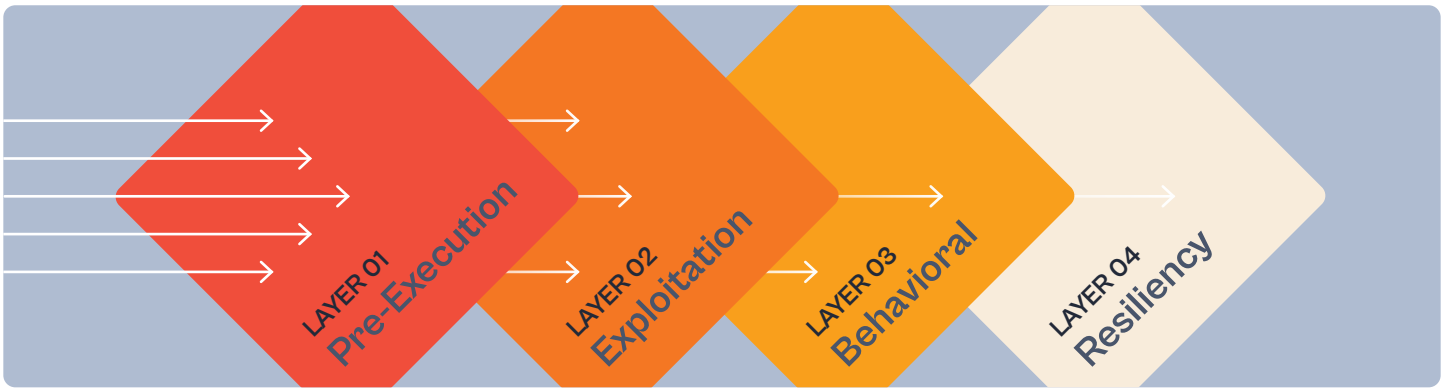
halcyon

Technical Deep Dive: Anti-Ransomware Protection

The *Halcyon Anti-Ransomware and Cyber Resilience Platform* was also designed with failure in mind: on the rare occasion that a ransomware payload manages to execute, Halcyon autonomously neutralizes the attack and enables teams to recover and restore the impacted endpoint quickly, within minutes.



Layer 01: Pre-Execution

Our Pre-Execution layer is the first line of defense and was built after dissecting millions of real-world ransomware attacks. By extracting the techniques, tactics, and procedures of these attacks and building machine learning micro-models to learn from them, the Halcyon platform is able to prevent ransomware execution from any point in the kill chain.

Layer 02: Exploitation

Ransomware operates within the confines of a ruleset to prevent it from being detected and to shield the operators from attribution. This protection layer enables the endpoint to exploit anti-analysis routines, laces the endpoint with artifacts to deceive the ransomware's internal execution rules, and creates a mirage to trigger and amplify malicious behavior. Layer 02 employs multiple methods of deception to detect ransomware processes and prevent ransomware from executing, including:

- **Geographic asset location and language deception techniques to trick ransomware into thinking it is running in a region it was coded to avoid (e.g.: Russia).**
- **Environmental deception techniques to make the endpoint appear as if it is a security tool used for analyzing malicious files such as virtualized sandboxing or debugging environments used for detonating binaries, or make the endpoint appear to be running a range of security products that the ransomware is designed to avoid triggering to remain stealthy.**
- **Forced conflict techniques to trick ransomware into thinking an asset is already compromised.**
- **File and process mirages, and services impersonation to make it appear as if the asset is of high value to elicit additional malicious behaviors from the ransomware that is detectable.**

Layer 03: Behavioral

Advanced and novel forms of ransomware are designed to circumvent security products like EPP, EDR, and XDR. They can generally detect when they are in controlled environments used for analysis and render those tools ineffective. Ransomware variants that can circumvent Layers 01 and 02 will trigger the protection offered by Halcyon's third layer due to its own deconfliction check attempts or in the process of initiating its core functions.

Most modern endpoint protection products leverage behavioral analysis – typically in the form of convolutional neural networks and decision tree algorithms – but these conventional machine learning capabilities still suffer from inherent flaws based on the size and complexity of the datasets required to train them and to remain contextually aware.

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

- **Allowing for data-driven supervised and unsupervised learning engines that work together across endpoints and the entire organization to analyze and convict suspicious processes in real-time.**
- **Delivering efficient analysis by leveraging several AI/ML models in parallel as opposed to relying on one monolithic detection model that may or may not be effective against a novel ransomware variant.**
- **Providing 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.**
- **Permits robust process tracing to detect and combat process injection to further harden against attacks against security products deployed on the system.**

Layer 04: Resiliency

Our multiple layers of protection are further backed by several levels of endpoint resiliency specifically designed to prevent a ransomware infection from spreading to other endpoints, reducing the potential impact of a successful ransomware attack. Halcyon employs several methods of reducing impact to an endpoint if a ransomware event occurs, including:

- **Ransomware encryption key capture and recovery that triggers any time uninitiated or potentially malicious encryption occurs on a system. This is paired with an automated universal decryptor to reduce recovery time from days to minutes.**
- **Hardening of Volume Shadow Service (VSS) to ensure that ransomware cannot delete or corrupt critical system backup snapshots.**
- **The Behavioral Layer and Resiliency Layer work in tandem to ensure if the detection of a malicious processes was missed in the previous layers, that recursive action can be taken to kill the process that is performing the malicious activity such as writing known malicious extensions to files.**

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 environments that have previously been compromised to prevent ransomware from executing.

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