halcyon

Technology Differentiation: Why the Halcyon Platform?

The Halcyon Advantage

Halcyon is the first contextually aware endpoint agent that prevents catastrophic disruptions from ransomware attacks by providing protection against the most advanced and novel ransomware variants.

The ***Halcyon Anti-Ransomware and Cyber Resilience Platform*** is designed to compliment existing endpoint security products and enhance their capabilities. In fact, our solution can amplify weak signals generated by ransomware to help existing security products trigger earlier on malicious events.

Understanding The Difference

CONTEXTUAL AWARENESS

Problem: Other products look at system processes through discrete inspections where they pass/fail each independent inspection, yet they do not carry any of the inspection intelligence over from one detection engine to the next, making evasion of those security tools much easier.

Solution: Halcyon weights trust based on a combination of attributes and behaviors to determine good, bad, or suspicious activity. We then carry that intelligence over through multiple inspection layers to formulate a high-fidelity detection based on correlating multiple sources of telemetry. This allows us to more quickly determine if an event is potentially malicious, so evasion is much more difficult for the attacker.

CONTINUOUS PRE-EXECUTION IMPROVEMENTS

Problem: Typically detection and prevention logic updates are manual and performed monthly or quarterly. This is too cumbersome and infrequent of a process to keep pace with attackers in a dynamic and ever-evolving threat landscape.

Solution: Halcyon delivers an autonomous solution that continuously corrects itself against a false negative result in a matter of minutes. We consider failing to block ransomware at the Pre-Execution layer a miss. When a threat is caught at any subsequent layer of protection, our solution automatically informs and updates the Pre-Execution layer so the variant cannot evade that first layer of protection again.

HALCYON FEATURES:

- Four layers of ransomware prevention and protection:
  - Pre-Execution
  - Exploitation
  - Behavioral
  - Resiliency
- Exceptionally low system resource consumption
- Supports Windows 10 & 11, Windows Server: 2012 R2, 2016, 2019, 2022
- Simple deployment with no reboots required

THE HALCYON STORY

Based in Austin, TX, Halcyon was founded in 2021 by a team of cyber 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 and other advanced threats.

CATASTROPHIC FAILURE

Problem: Endpoint protection solutions attempt to eliminate all threats all the time. However, they often struggle to detect ransomware, and the consequences result in catastrophic failure for the organization. The compromised endpoint or fleet of endpoints causes serious impact to the business, and the time to response and recovery increases dramatically along with the associated costs.

Solution: Halcyon has built resilience into the endpoint and designed an architecture that in most cases can eliminate the business impact stemming from a ransomware attack.

Key Use Cases

DETECTING AND PREVENTING RANSOMWARE

The Halcyon Platform fills the current ransomware protection gap, protecting against both known and novel ransomware variants with four layers of protection:

- **Pre-Execution**
- **Exploitation**
- **Behavioral Convictions**
- **Endpoint Resiliency**

IMPROVE SECURITY STACK EFFICACY

- Our protective kernel architecture protects current endpoint security tools from being blinded, unhooked, or uninstalled by ransomware, as well as amplifying bad behaviors to bolster their detections.
- If no endpoint security solution is active, Halcyon can enable Windows Defender (and select other products) and ensure it is up to date.

ENDPOINT RESILIENCE

- Halcyon eliminates the business impact of ransomware attacks by delivering automated recovery in minutes or hours as opposed to days and weeks.
- Our platform captures keys generated during a ransomware attack, removing the need to pay criminals to regain access.

Key Differentiators

OFFENSIVE MINDSET:

- The Halcyon Platform was designed around the attacker mindset because it was built by exploitation experts.
- Our layered control fabric delivers resilience because the platform was built with failure in mind.
- The platform was built with business impact in mind and substantially reduces – and in most cases eliminates – business impact entirely.
- Speed and context are everything, and the Halcyon Platform provides exceptionally high efficiency as ransomware eliminated by multiple detection engines that maintain deep contextual correlations from each preceding layer.
- Offensive techniques have been built into a defensive product to exploit the exploits for high fidelity detections earlier in the attack sequence.

TRULY INTELLIGENT SECURITY

- **Agile:** The Halcyon Platform was designed to be agile by way of its modular architecture, unlike traditional monolithic code bases that lack agility.
- **Adaptive:** Attackers will find ways to evade security controls, but our adaptive logic allows for swift retooling or the addition of new tooling in real-time to prevent new bypass techniques with no impact to product stability.
- **Aware:** As the Halcyon solution catches ransomware at any layer after Pre-Execution, it sends intelligence back to the Pre-Execution layer so it can detect and block that variant.

AI/ML MICRO MODELS

- AI/ML micro-models interrogate smaller subsets of data with extremely high fidelity and intercommunicate using the client environment as a distributed brain.
- These models are incredibly flexible and can adapt rapidly to baseline changes in the environment in comparison to the “slow to change” nature of convolutional neural nets and deep learning brains.

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!