halcyon

Better Together: Microsoft Defender + The Halcyon Anti-Ransomware Platform

Enhanced Zero-Day Ransomware and Data Exfiltration Protection with Halcyon + MS Defender

As ransomware and data exfiltration attacks evolve, the combination of Microsoft Defender and Halcyon offers comprehensive protection, ensuring detection, prevention, and rapid recovery from even the most advanced threats.

Key Benefits of combining Microsoft Defender and the Halcyon Anti-Ransomware Platform:

Focused Zero-Day Ransomware Blocking:

- Halcyon provides dedicated protection against zero-day ransomware binaries, addressing gaps that traditional solutions like NGAV, EDR and XDR tend to miss.
- This added layer ensures that even novel ransomware threats are blocked before they can cause harm.

Advanced File I/O and File-Less Attack Mitigation:

- While Microsoft Defender excels at blocking malicious activities involving both file-based and file-less attack vectors, the Halcyon Data Exfiltration Prevention (DXP) feature extends those protections.
- Halcyon detects and blocks attempts to transfer sensitive data, including exfiltration that may be delivered to malicious destinations via binary files or scripts.

Key Material Capture for Enhanced Resilience:

- In the event ransomware bypasses both Microsoft Defender and Halcyon prevention layers and executes on the targeted device, Halcyon captures the encryption key material and autonomously restores the device to operational.
- This unique Halcyon feature ensures encrypted data and devices can be quickly recovered without relying on threat actors to provide the decryption key, significantly improving recovery speed and resilience after a ransomware attack.

(Continued on next page)

HALCYON FEATURES:

- Four layers of ransomware prevention and protection:
  - Pre-Execution
  - Exploitation
  - Behavioral
  - Resiliency
- Exceptionally 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 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.

Proactive Tamper Resistance and Real-Time Alerts:

- Halcyon prevents unauthorized tampering with Microsoft Defender and other endpoint solution controls to ensure that critical defenses remain active and intact even if an attacker attempts to disable, unhook, or modify to bypass them completely.
- If Microsoft Defender engines are tampered with or disabled, Halcyon provides real-time alerts to security teams, enabling immediate investigation and response to potential threats.

Comprehensive Threat Monitoring and Active Response:

- Leveraging Microsoft Sentinel, organizations can automate responses and centralize threat insights from both Defender and Halcyon.
- This provides real-time protection against ransomware and data exfiltration attempts, whether delivered through file-based attacks, binaries, or network traffic.

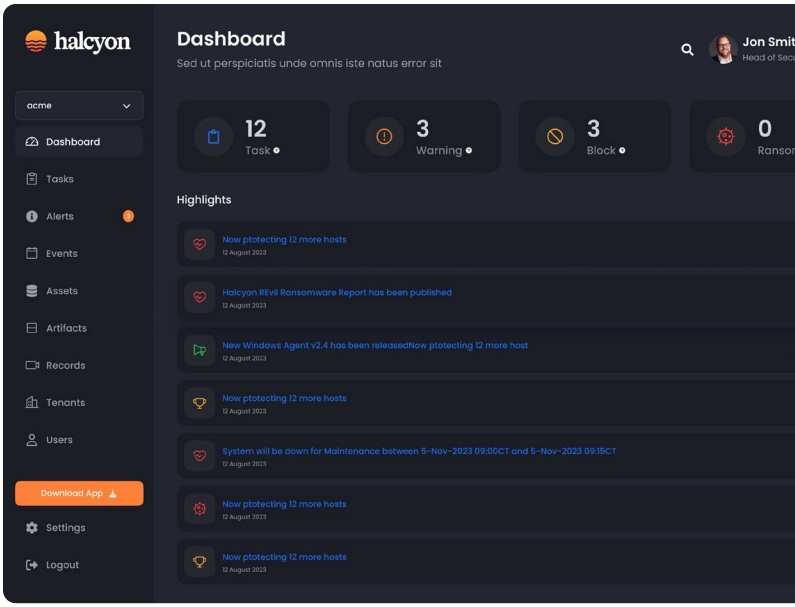

Fig 1: Halcyon Platform – Web Dashboard

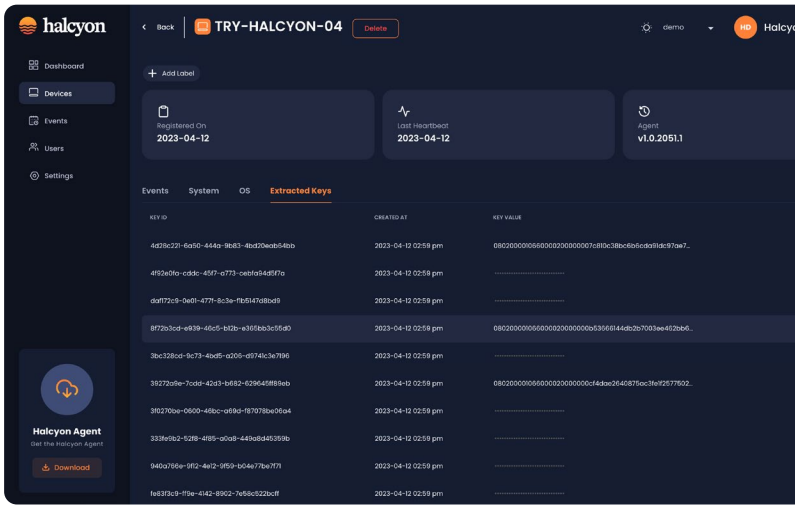

Fig 2: Halcyon Platform – Extracted Keys from Devices

In Summary: Halcyon + MS Defender Equals Complete Coverage

Together, Microsoft Defender and Halcyon deliver a robust, multi-layered defense strategy that protects against ransomware, binary-based data exfiltration, and other advanced cyber threats, ensuring comprehensive coverage and fast recovery.

Halcyon.ai is the leading anti-ransomware company that closes endpoint protection gaps and defeats ransomware through built-in bypass and evasion protection, key material capture, automated decryption, and data exfiltration prevention – talk to a Halcyon expert today **to find out more.**