halcyon

Data Sheet

Microsoft Defender + The Halcyon Platform Gives You Comprehensive Ransomware Protection

Enhance Your Ransomware Security with The Halcyon Anti-Ransomware Platform

As ransomware attacks evolve, the combination of Microsoft Defender for Endpoint and Halcyon delivers the comprehensive protection organizations need to ensure detection, prevention, and rapid recovery from even the most advanced ransomware attacks.

Key Benefits

Comprehensive Ransomware Protection:

Halcyon provides comprehensive ransomware protection across all stages of an attack, closing the gaps left by traditional solutions like NGAV, EDR, and XDR, commonly exploited by ransomware actors. Halcyon's ransomware protection complements Microsoft Defender's breadth of protection without creating additional work for your security team.

Ransomware Attack Associated Data Exfiltration:

Halcyon's Data Exfiltration Prevention ensures that ransomware actors cannot steal your organization's sensitive data. When data movement to a known nefarious site or data movement exceeding your pre-configured threshold is detected, Halcyon generates an alert that can be shared with Microsoft Defender XDR®, Microsoft Sentinel,® or any other SecOps platform for immediate investigation and response.

Encryption Key Material Capture for Enhanced Resilience:

When Halcyon detects ransomware-initiated encryption on a protected asset, the platform automatically intercepts encryption key material, enabling fast data recovery without negotiating with the attackers. 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.

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

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 Arctic Wolf®), 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 of the Microsoft Defender agent/service and other endpoint security controls to ensure critical defenses remain active and intact when an attacker attempts to disable, unhook, or bypass them altogether.

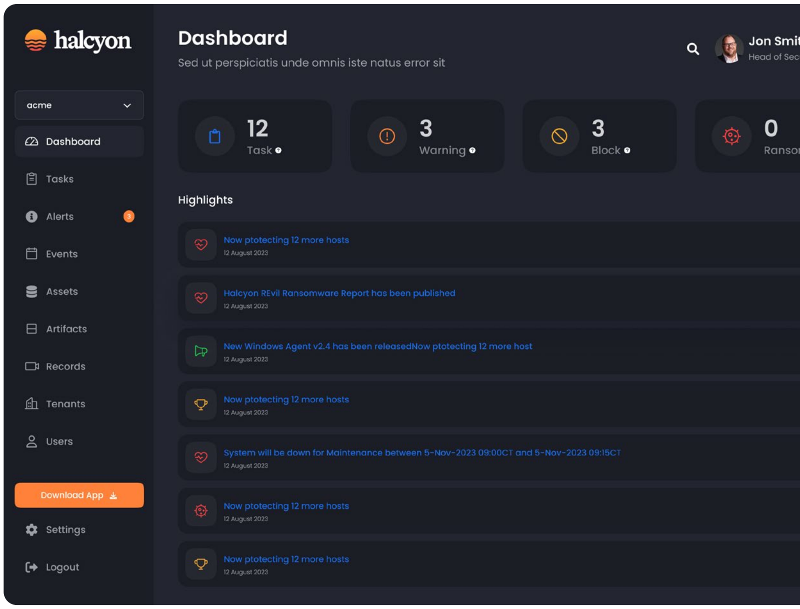
If Microsoft Defender is tampered with or disabled, Halcyon provides real-time alerts to security teams, enabling immediate investigation and response to potential threats.

Comprehensive Threat Monitoring and Active Response:

Organizations can centralize investigation and automate responses to alerts from Microsoft Defender, Halcyon, and any other security control using Microsoft Defender XDR® or Microsoft Sentinel.® This provides real-time protection against ransomware and data exfiltration attempts, whether delivered through file-based attacks, binaries, or network traffic.

Halcyon + Microsoft Deliver Complete Ransomware Protection.

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



Dashboard

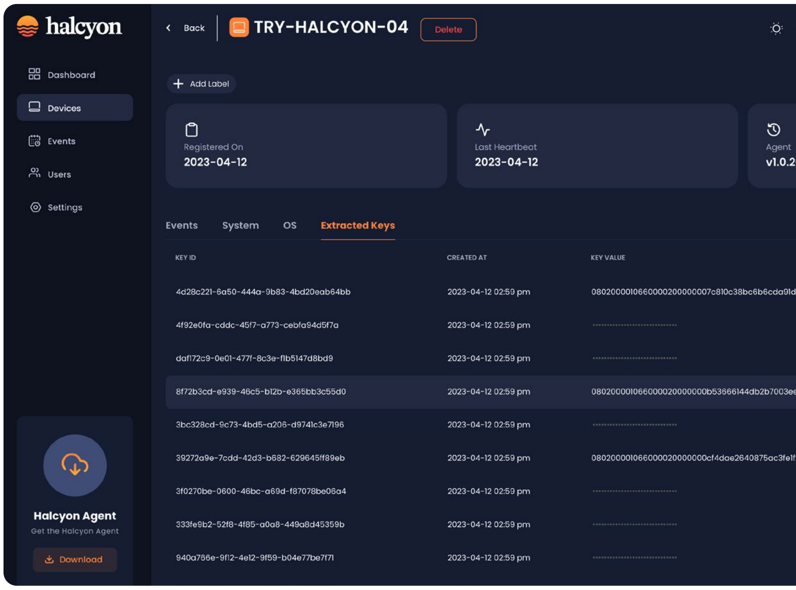
Sed ut perspiciatis unde omnis iste natus error sit

12 Task · 3 Warning · 3 Block · 0 Ranso

Highlights

- Now ptotecting 12 more hosts — 12 August 2023
- Halcyon REvil Ransomware Report has been published — 12 August 2023
- New Windows Agent v2.4 has been releasedNow ptotecting 12 more host — 12 August 2023
- Now ptotecting 12 more hosts — 12 August 2023
- System will be down for Maintenance between 5-Nov-2023 09:00CT and 5-Nov-2023 09:15CT — 12 August 2023
- Now ptotecting 12 more hosts — 12 August 2023
- Now ptotecting 12 more hosts — 12 August 2023

Fig 1: Halcyon Platform – Web Dashboard



TRY-HALCYON-04

Registered On: 2023-04-12

Last Heartbeat: 2023-04-12

Agent: v1.0.2

KEY ID	CREATED AT	KEY VALUE
4d28c221-6a50-444a-9b83-4bd20eab64bb	2023-04-12 02:59 pm	080200001066000020000000 7c810c38bc6b6cda91d
4f92e0fa-cddc-45f7-a773-cebfa94d5f7a	2023-04-12 02:59 pm	••••••••••••••••••••••••••••
daf172c9-0e01-477f-8c3e-f1b5147d8bd9	2023-04-12 02:59 pm	••••••••••••••••••••••••••••
8f72b3cd-e939-46c5-b12b-e365bb3c55d0	2023-04-12 02:59 pm	0802000010660000200000000b53666144db2b7003e
3bc328cd-9c73-4bd5-a206-d9741c3e7196	2023-04-12 02:59 pm	••••••••••••••••••••••••••••
39272a9e-7cdd-42d3-b682-629645ff89eb	2023-04-12 02:59 pm	080200001066000020000000cf4dae2640875ac3fe1f
3f0270be-0600-46bc-a69d-f87078be06a4	2023-04-12 02:59 pm	••••••••••••••••••••••••••••
333fe9b2-52f8-4f85-a0a8-449a8d45359b	2023-04-12 02:59 pm	••••••••••••••••••••••••••••
940a766e-9f12-4e12-9f59-b04e77be7f71	2023-04-12 02:59 pm	••••••••••••••••••••••••••••

Fig 2: Halcyon Platform – Extracted Keys from Devices

See the Halcyon Difference for Yourself

The threat of a successful ransomware attack impacting your organization has never been higher. With Halcyon and Microsoft Defender working together, you get the comprehensive ransomware protection you need to ensure your organization can withstand any ransomware attack it encounters today, tomorrow, and in the future. To see Halcyon in action, visit halcyon.ai and schedule a demo today!

Microsoft Defender for Endpoint, Microsoft Sentinel, and Microsoft Defender XDR are trademarks of Microsoft Corporation. Halcyon is not affiliated with, endorsed, or sponsored by Microsoft Corporation.

Get a demo at halcyon.ai/demo or sales@halcyon.ai