halcyon

Protecting Healthcare Providers From Ransomware

Ransomware attacks are the biggest threat facing organizations today, and healthcare providers have been hit particularly hard. Criminal ransomware groups know that the impact of an attack against healthcare organizations does not just disrupt everyday business, it directly affects the lives of their patients.

The recent ***Shields Up*** announcement from Cybersecurity and Infrastructure Security Agency (CISA) advised U.S. organizations to remain vigilant with respect to an increased risk from ransomware and destructive data attacks as a result of the Russian invasion of Ukraine and lie likelihood that ransomware attacks against Western targets are likely to escalate.

Legacy security tools were simply not designed to address the unique threat that ransomware presents, and this is why we keep seeing destructive ransomware attacks circumvent these traditional security solutions.

That is why we enlisted some of the top data scientists and threat researchers in the security field to develop the *Halcyon Anti-Ransomware and Cyber Resilience Platform* – the first and only self-healing, purpose-built ransomware prevention solution that hardens endpoints against how ransomware actually works.

The Challenges

Ransomware poses several challenges to any healthcare provider:

People & Process – Most ransomware events start with a human entry point. Whether it's social engineering, phishing, accidental misconfiguration, or a rogue insider – people and processes are what cybercriminals use to gain access to a system. Legacy technical debt, underfunded programs, and non-investment in skilled resources leave openings throughout the IT stack for attackers to leverage.

Motivations – Ransomware groups are organized, competent, and motivated by profit. They quickly adapt to changing conditions and only must be right once – defenders need to be right every time.

Downtime – From when it is first detected to when recovery is complete, an organization needs 7 – 21 days to restore normal operating conditions from a ransomware attack. That is weeks of degraded services to patients, providers and families with lives potentially at stake.

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.

Ransomware Stats in Healthcare:

755% increase in healthcare cyberattacks in 2021

39+ ransomware crime groups specifically targeted healthcare

$20 Billion in cost to healthcare in 2020 alone

Building Resilience

The new model of building resilient organizations requires:

- **Defense Resilience –** Existing EPP, EDR, and XDR is not built to stop ransomware. Halcyon's AI is trained on millions of real-world ransomware incidents to plug detection and prevention gaps left by traditional security tools.
    - **Bypass and Evasion Prevention –** Modern attackers target popular security tools and leverage bypass techniques to disable and render them useless. Halcyon's unique architecture allows our platform to augment and armor all other security tools running on an endpoint and prevent them from being unhooked.
- **Operational Resilience –** Every minute a system is down from a ransomware attack it costs hard dollars. Halcyon has two key features that reduce the recovery time from ransomware from weeks down to minutes.
    - **Full Encryption Key Capture –** Our intelligent agent captures the encryption event, shuttles the keys into a secure enclave and, after the malicious process is blocked, automatically decrypts any impacted files on the endpoint. This eliminates the need to pay a ransom.
    - **Data Exfiltration (Q3 2023) –** Ransomware operators hide their data exfiltration extremely well and handily fool common data loss products. Halcyon's data exfiltration module extends the core capabilities to shut down attackers attempting to remove data to hold for ransom on a leak site.

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 info 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 consultation with a ransomware expert.