halcyon

Data Sheet

Halcyon Anti-Ransomware Platform is Closing the Ransomware Security Gap

The Ransomware Gap

While many organizations assume their endpoint security product, combined with their backup strategy, provides sufficient protection against ransomware attacks, the evolution of attackers' TTPs leaves organizations with a ransomware security gap.

Why Endpoint Security Products Fail to Stop Ransomware

Easily Bypassed: Ransomware actors use various techniques to bypass endpoint security products, leaving organizations unaware of the attacks until after encryption occurs and ransom demands are made.

Reactive Security: Endpoint products may eventually uncover an attack, but only after the attacker damages the environment, leaving the organization with an expensive recovery process.

The Rise of Multi-Extortion: Legacy endpoint security products cannot detect ransomware-initiated data exfiltration, leaving organizations open to multi-extortion attempts from attackers.

The **Halcyon Anti-Ransomware Platform** is the only endpoint security platform designed to combat modern ransomware across all stages of an attack, closing the ransomware security gap.

The Halcyon Platform

- Prevents ransomware-related files and processes from executing automatically
- Uncovers and stops ransomware behaviors during an active attack
- Recover encrypted data quickly without paying a ransom or using backups
- Includes 24/7/365 threat monitoring, investigation, response, and recovery service delivered by the Halcyon Ransomware Detection and Recovery (RDR) Team

With Halcyon, organizations can:

- Eliminate downtime and business disruption
- Avoid ransom payments
- Reduce ransomware risk

The Halcyon Advantage: Human Expertise

While many products claim to protect organizations from ransomware, the security team using the product must have significant ransomware expertise to reach the product's stated benefits. With Halcyon, organizations get the technology and human expertise to eliminate the threat of a successful ransomware attack. Every Halcyon deployment includes Halcyon Ransomware Detection and Recovery (RDR), powered by the Halcyon RISE Team, at no additional cost. This 24/7/365 specialty service monitors and acts on any ransomware-related event in your environment. With years of in-the-field experience combatting ransomware, Halcyon RDR ensures every customer gets the best protection from ransomware across all stages of an attack.

Designed to Work with Your Endpoint Security

We designed our platform to work seamlessly with any existing endpoint security product, including Microsoft Defender®, CrowdStrike Falcon®, Sentinel One Singularity™, and more. Since we focus on ransomware, we only detect, prevent, respond, and recover from ransomware-specific threats not

identified by your existing security product. This means you can be confident Halcyon will not cause duplicate alerts that could increase the workload on your security team. Halcyon alerts can also be easily integrated into any leading SIEM, XDR, and SOAR product, increasing security teams' ability to provide comprehensive ransomware protection across their environment.

Halcyon Capabilities

Before Attack

For security practitioners, the sooner an attack can be prevented, the better.

- **Pre-Execution Prevention Engine:** Using AI/ML models trained exclusively on ransomware, Halcyon can detect and prevent files and processes exhibiting ransomware attributes from executing, including never-before-seen and zero-day variants.

During Attack

Our unique understanding of how ransomware attackers operate allows us to uncover their behaviors, which other endpoint security products might mistake for normal user behavior.

- **Behavior Modelling:** When any process begins exhibiting known ransomware actor behaviors, we can stop it.
- **Agent Self Protections:** If the Halcyon agent is stopped unexpectedly, we automatically generate an alert to enable fast investigation and mitigation.
- **Sidekick Protection:** Halcyon detects any unexpected stopping of services related to Microsoft Defender®, CrowdStrike Falcon®, and SentinelOne Singularity™ products, ensuring attackers cannot gain further access to the system and environment.
- **Data Exfiltration Prevention:** Ransomware-tuned data protection engine that automatically detects data exfiltration to known malicious sites commonly used by ransomware actors.
- **Encryption Key Material Intercept:** Automatically captures encryption key material during a ransomware encryption event, enabling the swift recovery of any encrypted data.

After Attack

With extensive in-the-field ransomware security experience, Halcyon can rapidly assess any strain of ransomware and identify what can be done to restore your organization to normal operations.

- **Data Decryption:** When Halcyon detects ransomware-initiated data encryption occurs, Halcyon will use the captured encrypted key material and in-depth knowledge of ransomware encryption methods to deploy a decryptor to the endpoints to decrypt the data.
- **Recovery and Restoration:** After data decryption on the initial impacted assets, Halcyon will work to deploy decryptors across the entire environment to ensure no other assets were affected by the attack, restoring the environment to a pre-attack state.

The Halcyon Ransomware Warranty

Halcyon customers with the solution fully deployed have yet to experience a widespread ransomware attack, but we know it could happen. To that end, every Halcyon customer receives a no-cost ransomware warranty. If you experience a ransomware attack in your fully Halcyon-protected environment, the Halcyon RISE team will work with your security team to quickly return your environment to normal operations.

The Bottom Line

While all successful cyberattacks can leave your security team scrambling, ransomware attacks are the most damaging, with long-lasting impacts. Halcyon lives and breathes ransomware and is the only company combining technology with human expertise that can, once and for all, remove ransomware from your list of things keeping you up at night. Visit Halcyon.ai today to set up a personalized demo.