TECHNICAL VALIDATION

Halcyon Anti-Ransomware Platform

Closing the Gap Between Endpoint Detection and Recovery

By Alex Arcilla, Principal Analyst – Validation Services
Omdia

FEBUARY 2026

Contents

Introduction

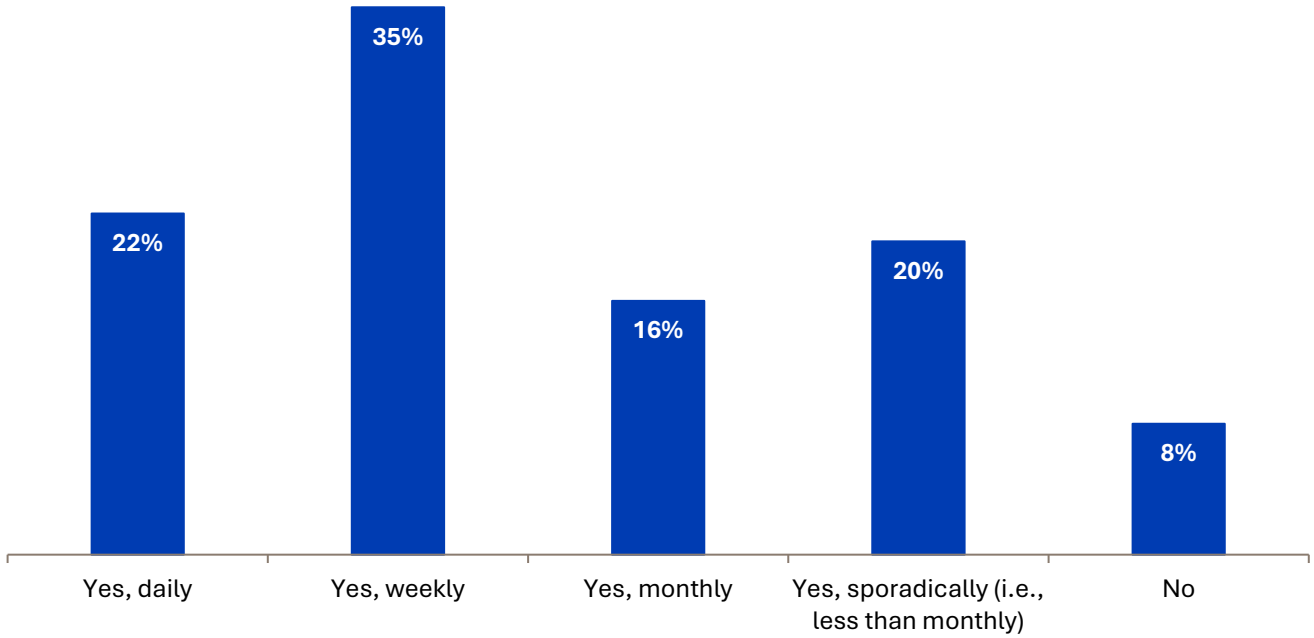
This Omdia Technical Validation evaluates how organizations can use the Halcyon Anti-Ransomware Platform to improve their security posture against ransomware. We review how the platform can detect and disrupt ransomware faster and more effectively than commonly used tools and approaches, leading to increased cyber resiliency and faster business recovery.

Background

Ransomware is not going away; Omdia research found that 57% of surveyed respondents considered ransomware to be amongst the top three threats to their organization's health compared to other risks.[1] And over half of respondents stated that, in the past year, their organizations have experienced attempted ransomware attacks daily or weekly (see Figure 1).

Figure 1. Frequency of Ransomware Attacks Experienced in the Past Year

Has your organization experienced an attempted ransomware attack within the last 12 months? (Percent of respondents, N=400)



Source: Omdia

Although organizations state they are prepared to deal with ransomware attacks, our research shows that this may not be the case. Ninety-five percent stated that they did not thwart ransomware attacks in the past year, causing real damage such as lost or encrypted data and operational downtime. Additionally, more than two-thirds of organizations reported that they paid the ransom to regain access to their data, applications, or systems. Moreover, nearly nine out of 10 organizations received additional extortion attempts beyond the initial ransomware demand, and nearly two-thirds of those organizations reported satisfying the additional

[1] Source: Omdia Research Report, *The Ransomware Reality: Cyber Resilience, Data Resilience, and Data Protection*, November 2025. All Omdia research references and charts in this Technical Validation are from this report.

demands (see Figure 2). This illustrates how devastating data exfiltration and double extortion methods can be, as organizations want to avoid potential financial losses or loss of customer trust and brand reputation.

Figure 2. Impacts of Double Extortion Methods

Source: Omdia

While endpoint detection and response (EDR) solutions have been used in the fight against ransomware, they may not be designed to actually deal with the nature of ransomware. Like most security tools, EDR tools are developed to detect any threat or attack. Yet, they are not specifically designed to identify evidence of ransomware. Additionally, EDR solutions operate in a reactive mode, but reacting to a ransomware attack is "too late," as the damage has already occurred.

Since ransomware continuously evolves, these attacks can avoid EDR detection by leveraging EDR bypass and disabling techniques. These controls focus on known and persistent behavior from bad actors (e.g., nation-states). Ransomware can also rely on credential theft and the escalation of existing access privileges, which EDR solutions already use to verify identities. Some ransomware attacks do not even attempt to bypass EDR solutions, with legitimate tools used for everyday tasks (e.g., remote monitoring) actually facilitating an attack campaign, which can then go undetected.

Many organizations are dealing with ransomware attacks from a backup and recovery perspective. While the attack has already occurred, organizations have determined that the best way to protect themselves is to create backups continuously, then recover using those backups if needed. However, a recovery may take longer than expected (days to weeks), and there is no guarantee that all data will be recovered. In fact, attackers often delete backups.

SecOps teams are overwhelmed with alert fatigue and false positives but still need to address ransomware successfully to prevent their organizations from experiencing additional security risk, as well as increased financial and business risk.

Halcyon Anti-Ransomware Platform

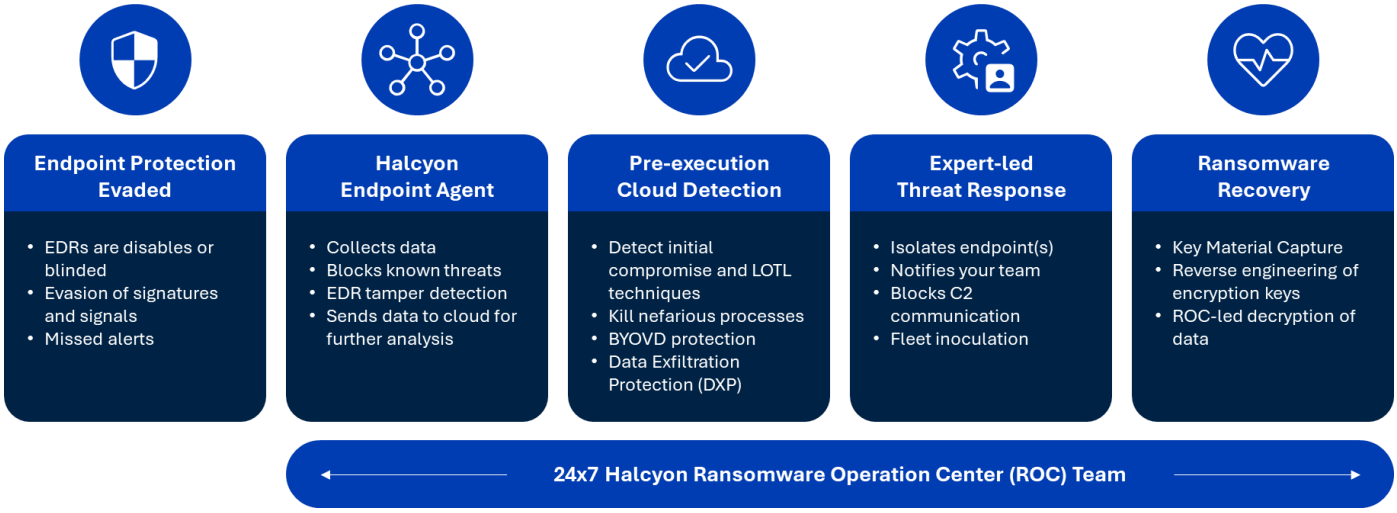
Halcyon offers a purpose-built platform that provides 24/7 monitoring and coverage to existing SecOps teams for ransomware attack protection. The platform supports detection, triage, investigation, response, eviction, and recovery when ransomware attacks occur. Unlike other security tools, Halcyon focuses on detection and

response, using ransomware evasion techniques, such as bring-your-own-virtual-device (BYOVD), EDR tampering, and living off the land.

Halcyon operates via an agent-cloud model (see Figure 3), with a lightweight endpoint agent sitting behind the EDR solution. If the agent detects a potential anomaly that has bypassed EDR controls, it will be sent to the Halcyon cloud and evaluated by the platform's AI/ML models, trained on ransomware behaviors, to determine if evidence of ransomware exists. If the Halcyon cloud determines that ransomware is present, an alert is sent, and the appropriate remediation is sent to the infected machine.

If the response is not sent in time to evict the threat, a series of behavioral analyses take place at the host level. If the host detects any evidence of ransomware, the machine is isolated. Because the Halcyon cloud and agent work in parallel, organizations no longer need to worry about the same attack happening again, as the platform can recognize ransomware behavior and evict it before it executes. In other words, that attack will only be executed once, removing the risk of repeated attempts.

Figure 3. How the Halcyon Anti-Ransomware Platform Works



Source: Halcyon and Omdia

Behind the platform is a 24/7 ransomware SOC—the Halcyon Ransomware Operations Center (ROC) team—that delivers the expertise and coverage for stopping ransomware before it inflicts damage. If data has been encrypted, the ROC team assists in recovery operations, helping the affected organization recover as quickly as possible. With Halcyon's included recovery and services warranty, the ROC team also provides incident response until organizations are operating normally and all traces of the ransomware attack have been evicted.

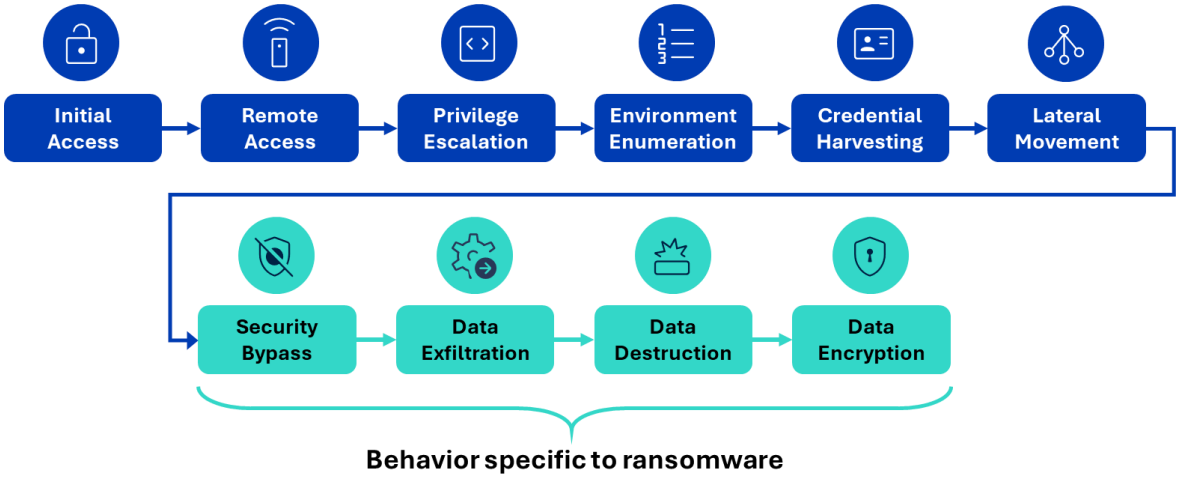
The combination of the agent-cloud model, behavioral analysis, AI/ML engines, and the Halcyon ROC team enables this platform to detect and respond to ransomware attacks in a matter of seconds. Given the speed at which an attack can destroy and encrypt data, the platform has been developed to operate more quickly than any SecOps team could manually attempt to isolate or recover from ransomware, minimizing financial loss and unwanted downtime.

Omdia Technical Validation

Omdia validated, through briefings and online demonstrations, how the Halcyon Anti-Ransomware Platform can help organizations, specifically their SecOps teams, improve their ability to detect and respond accordingly to ransomware attacks faster than EDR solutions. We specifically focused on the areas in which the platform augments an organization's EDR tool to identify and contain specific behaviors that indicate the presence of ransomware.

The platform is equipped to stop ransomware at any step in the "kill chain," the sequence of behaviors associated with ransomware (see Figure 4). Halcyon works to limit the progression of that kill chain as early as possible. The platform is also designed to detect pre-ransomware behavior to prevent the attack from progressing along the chain (e.g., raising an alert when encountering anomalous remote access). When ransomware is detected, Halcyon works to evict the threat actor.

Figure 4. Ransomware Kill Chain



Source: Halcyon and Omdia

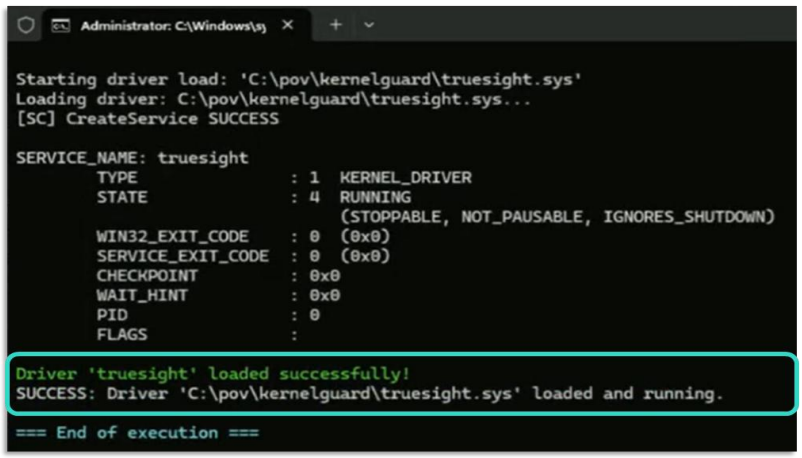
While EDR tools have capabilities to detect some techniques in the kill chain, not all are covered. Halcyon has implemented additional capabilities for detecting and isolating suspicious activity related to three steps specific to ransomware attacks: security bypass, data exfiltration, and data destruction/encryption.

Security Bypass

Threat actors can bypass security by stealing credentials that enable their encryptors to pass undetected. Other methods can be used for security bypass, such as compromised drivers to gain kernel-level access and disabling existing security controls, such as BYOVD, or injecting malicious code into executable files.

Omdia reviewed how Halcyon detects attempts at security bypass. We uploaded and executed a BYOVD using the file "BYOVD_demo.exe" into an environment containing a Halcyon agent (see Figure 5). If undetected, the executable was designed to disable an organization's EDR solution.

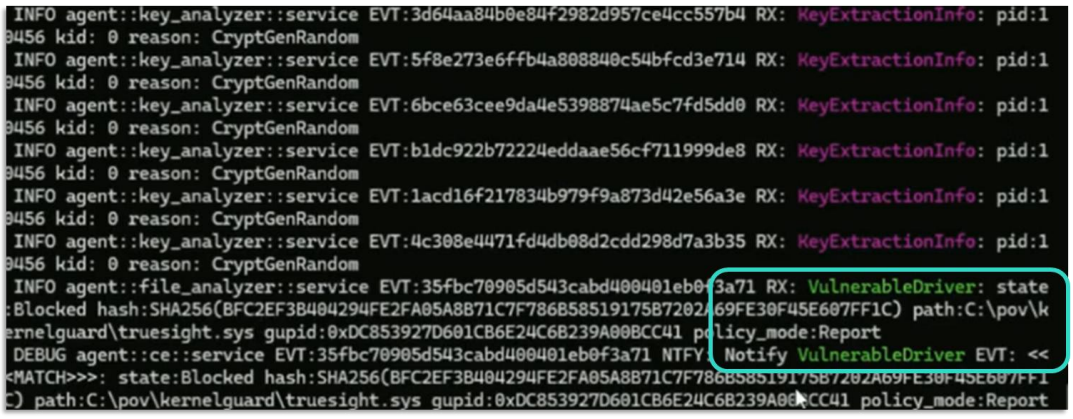
Figure 5. Successful Upload of BYOVD



Source: Omdia

After the Halcyon agent transmitted some logs to the Halcyon cloud, Omdia observed that an alert was raised in a matter of seconds (see Figure 6).

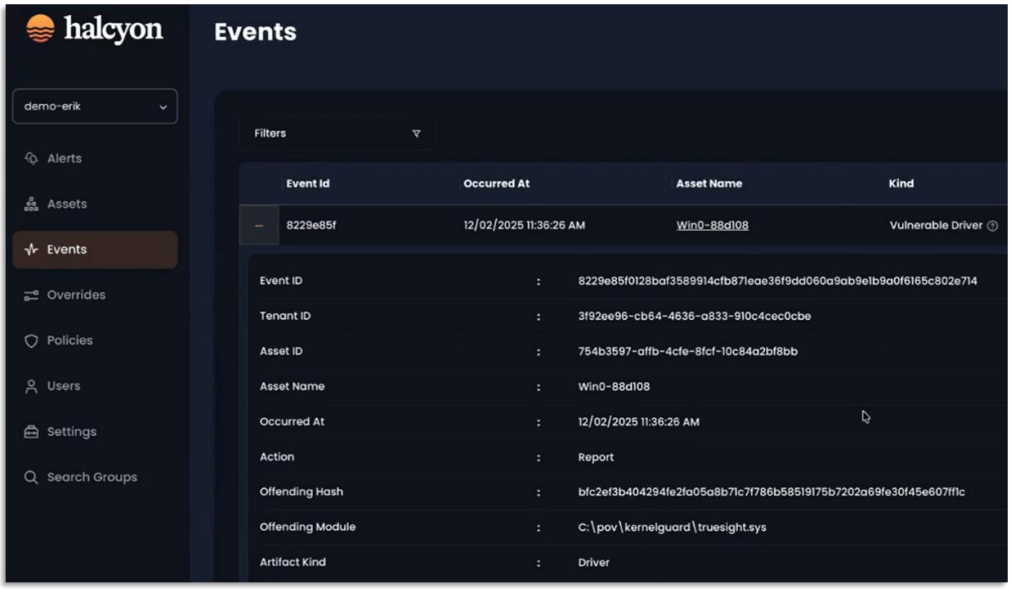
Figure 6. Detection of "Vulnerable Driver" Security Bypass



Source: Omdia

Halcyon recorded the event as shown in Figure 7. An alert is delivered to both the customer and the ROC team via the Halcyon console. Once the ROC team receives the alert, work begins on isolating and evicting the attack.

Figure 7. Alert of Security Bypass Event



Source: Omdia

Omdia should note that an indication of this type of event deserves attention if the platform has been operational within a customer's IT environment for some time. If the platform is newly deployed, Halcyon detects "vulnerable drivers" because of the existing attack surface. During implementation, these turn out to be outdated files, most likely not containing security patches, that have resided in the environment and have never been replaced. Therefore, they most likely are "false positives." Once those files have been removed, the probability is high that detecting this event is a positive result requiring immediate attention.

Why This Matters

The importance of detecting security bypass attempts is critical. If a bad actor can complete that step of the ransomware kill chain, attempts at data exfiltration will start within milliseconds.

Omdia validated that the Halcyon Anti-Ransomware Platform can detect and isolate security bypass events, such as BYOVD. We observed how the Halcyon agent sends logs and relevant data to the Halcyon cloud, which are processed and examined using the platform's AI/ML engine to recognize the incident as a BYOVD event in seconds. This speed is critical so that the Halcyon ROC team can work on isolation and removal to stop the ransomware attack.

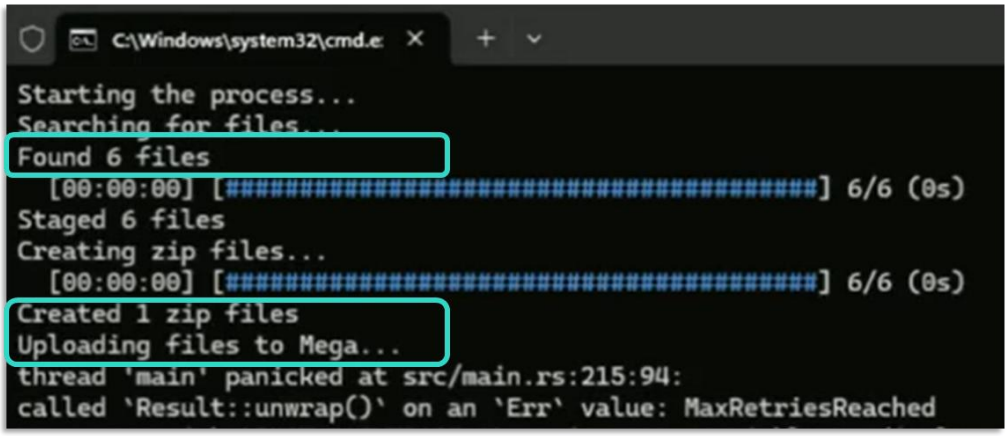
Data Exfiltration

Threat actors have found that using scripts is an easy and fast way to execute a ransomware attack. To perform a data exfiltration, a ransomware attack typically sends data to cloud-based infrastructure (e.g., MEGA[2], Cloudflare) or a grey FTP site. To detect attempts at data exfiltration, Halcyon focuses on identifying events in which any amount of data is sent somewhere outside of the organization's environment.

[2] MEGA (Mega Encrypted Global Access) is encrypted cloud storage.

To observe how Halcyon detects data exfiltration, six files were uploaded and stored in a .zip file. We began uploading the .zip file to MEGA (see Figure 8).

Figure 8. Example of Data Exfiltration: Uploading Data to MEGA



Source: Omdia

Halcyon looks for evidence of data exfiltration events by noting unusual DNS queries (e.g., if data is being sent to unusual locations) and measuring how much data is transmitted with volumetric alerts. Omdia observed that the Halcyon agent sent logs until flagging the detection of "Bad IP address" and revealing the data's destination as MEGA (see Figure 9).

Figure 9. Detection of Data Exfiltrated to MEGA

Source: Omdia

Detecting this type of security event using manual methods would obviously consume more time and effort than SecOps teams can spare. Once exfiltration is detected, SecOps teams do not have the resources to respond quickly enough, as data can be encrypted and stolen within milliseconds.

Why This Matters

Any detection of data exfiltration requires a response in seconds before encryption begins. SecOps teams do not have the bandwidth or experience to conduct this type of investigation at the speed required to isolate the attack.

Omdia validated that the Halcyon Anti-Ransomware Platform can detect data exfiltration attempts in a few seconds. We observed how the platform leveraged DNS monitoring and volumetric alerts to flag unusual amounts of data sent to sites typically used by bad actors for parking stolen data, such as MEGA and Cloudflare. By observing this process, Omdia confirmed the speed at which Halcyon detects data exfiltration attempts, which far surpasses the speed of completing this analysis manually.

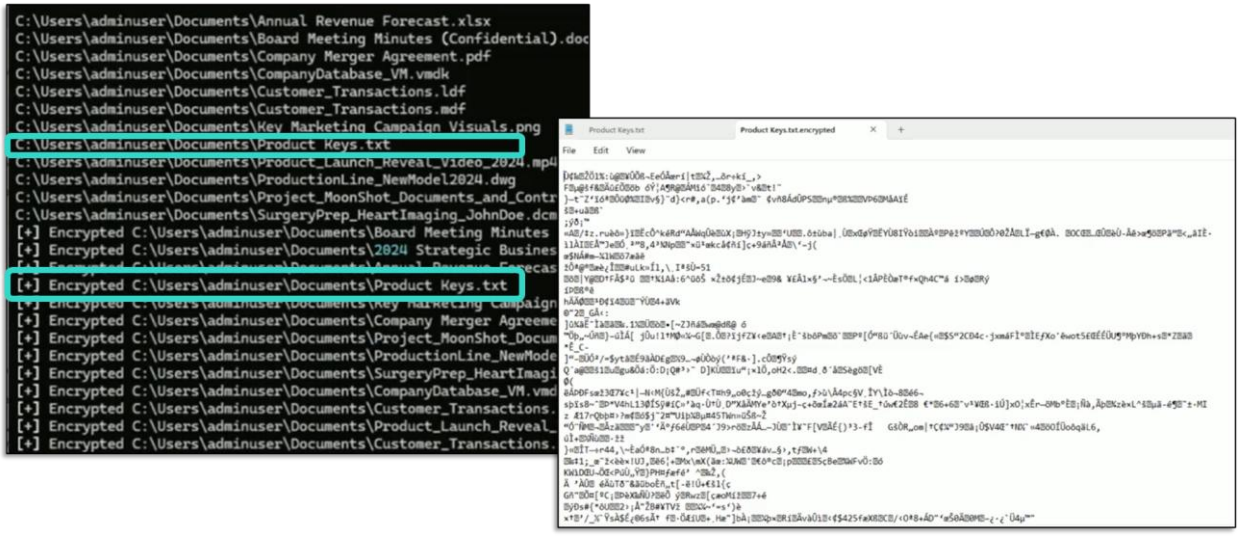
Data Destruction/Encryption

If the ransomware attack has progressed to the data destruction and encryption stage, many organizations believe that they have little recourse but to give in to the ransom demands and resign themselves to recovery. The financial damage not only comes from paying the ransom but also from lost business due to unplanned downtime; recovery can occur over days or weeks before organizations are back to normal operations. On the other hand, Halcyon can help organizations find some recourse that minimizes the financial damage while speeding up recovery.

Should data encryption occur, Halcyon assists in data recovery by leveraging the encryption keys associated with the attack. With key material interception, the Halcyon platform retrieves the symmetric keys used, along with the encrypted file and the encryption algorithm. The Halcyon ROC team then "reverse engineers" the keys to develop a decryptor, usually in less time than is needed to completely evict the ransomware threat.

Figure 10 shows the data in a file named "Product Keys.txt" encrypted using Akira. The encrypted data is also displayed.

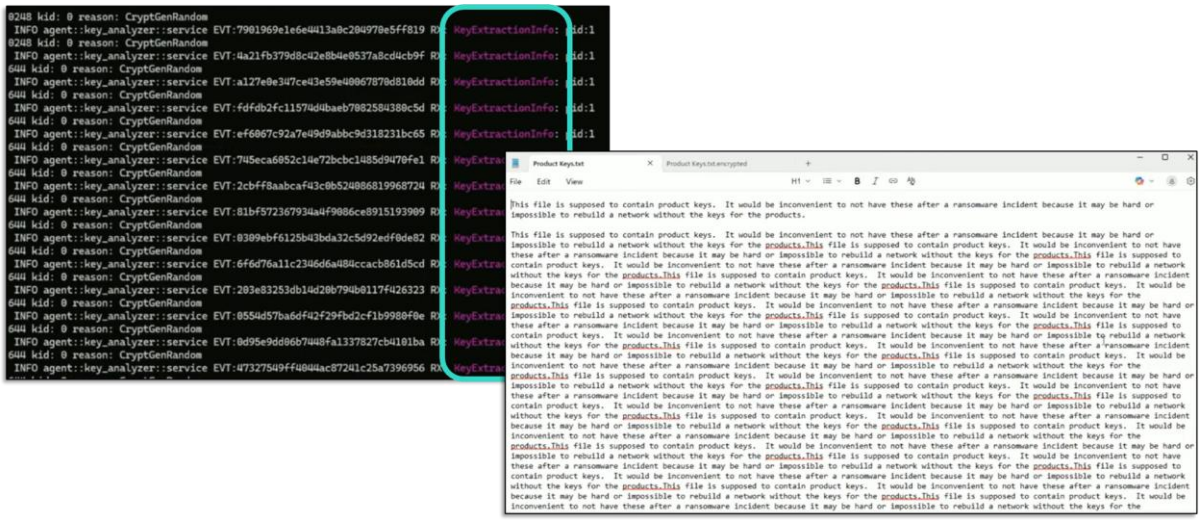
Figure 10. Encryption via Akira Ransomware



Source: Omdia

Once the Halcyon cloud retrieved the keys, a decryptor, "KeyExtractionInfo," was developed and deployed to all endpoints, not just the host machine in which the ransomware attack occurred (see Figure 11).

Figure 11. Deploying Decryptors



Source: Omdia

As Omdia observed how Halcyon supports data recovery, we noted that this approach can help to minimize the downtime organizations face after a successful ransomware attack. The decryptors help to maximize the amount of data retrieved, thus increasing the chances of returning to "business as usual." Again, the speed in which Halcyon can help reduce recovery time also decreases the operational overhead encountered when performing recovery operations using traditional methods.

Why This Matters

When a ransomware attack is successful in holding data hostage, organizations see little recourse and end up engaging in recovery operations that can last longer than desired. To add insult to injury, 45% of organizations reported recovering only half or less of their data. The operational and financial impacts can be significant.

Omdia validated that the Halcyon Anti-Ransomware Platform can reduce the time and data loss associated with recovering from a ransomware attack. We observed how the platform uses the bad actor's encryption keys to develop a decryptor that can increase the amount of recovered data. Combining this decryptor with the help of Halcyon's ROC team to completely evict the ransomware threat can help organizations decrease the operational overhead typically spent on recovery operations using typical approaches such as restoring from backup.

Conclusion

Ransomware continues to evolve, becoming more sophisticated in evading detection. In fact, over 40% of organizations reported that ransomware remained undetected in their environments for between eight and 30 days. While many organizations may believe that they are prepared to recover from a ransomware attack, less attention might be placed on detecting ransomware in the first place. While organizations use EDR tools, the amount of undetected ransomware calls into question the effectiveness of those solutions. Simply put, EDR

solutions are meant to detect and isolate any attack or threat, but they have not been designed to tune into the specific behaviors and approaches of ransomware attacks. Given the increasing business and financial risk that ransomware presents, the need for an alternative solution emerges.

The Halcyon Anti-Ransomware Platform is designed to detect and evict ransomware by focusing on the unique techniques and behaviors displayed when executing an attack. Unlike EDR tools, Halcyon uses a combination of behavioral analysis and AI/ML models, trained exclusively on ransomware, to isolate, stop, and evict ransomware. Organizations using Halcyon receive 24/7 support from its ROC team for ongoing investigation, alerts, response, and recovery (if needed). The goal is to stop ransomware attacks as early as possible, if not prevent them from infiltrating an environment and remaining undetected for extended periods of time.

Throughout our evaluation, Omdia validated that Halcyon can help protect organizations from ransomware by isolating and removing the threat at any stage in the ransomware kill chain. While Halcyon is designed to detect ransomware before infiltrating an organization, Omdia observed that the platform can also reduce the time and effort needed to address steps in the kill chain not covered by EDR, namely, security bypass, data exfiltration, and data destruction/encryption. In these cases, not only did Halcyon detect evidence of these actions, but it also isolated and eliminated the threat in a matter of seconds. We noted the speed at which Halcyon performed outpaced any manual efforts done by SecOps teams to realize the same result. The Halcyon platform's ability to work quickly reflects the urgency of dealing with ransomware, as these attacks can occur in a matter of seconds.

If ransomware concerns are overwhelming your existing SecOps team, and you want peace of mind from potential business and financial risk, Omdia urges you to consider the Halcyon Anti-Ransomware Platform as a part of your overall security strategy.

Get in touch: www.omdia.com askananalyst@omdia.com