whitepaper

Introductory Guide to Enterprise Ransomware Defense Strategy

www.halcyon.ai

halcyon

Table of Contents

01 Understanding Modern Ransomware Operations

Ransomware is fundamentally different from other forms of malware as it is purposely disruptive to an organization. General Remote Access Trojans (RATs) provide ingress into networks, and info stealers exfiltrate sensitive data, but neither grind business operations to a halt.

Ransomware is no longer considered just a technical threat, but rather the largest single risk to any organization. According to research from 2022, **85% of companies are the victim of at least one ransomware attack per year, and 74% have experienced multiple attacks.**

Current endpoint protection solutions available on the market, while robust and effective for many threats, do not fully protect against ransomware attacks because they were designed to find and block commodity malware.

Ransomware groups, known as Ransomware-as-a-Service (RaaS) operators, are implementing novel advanced evasion techniques into their payloads specifically designed to evade or completely circumvent traditional endpoint protection solutions.

IMPACT TO VICTIM ORGANIZATIONS

On average, a ransomware attack took 237 days to detect and 89 days to fully remediate. The annual impact from ransomware attacks in the US alone is estimated to be more than $20 billion dollars. Remediation costs following a ransomware attack average more than $4M per incident per each targeted organization.

This figure does not include additional incident response costs, tangential costs, damage to the brand, lost revenue, lost production from downed systems, and other collateral damage:

The first half of 2022 saw an estimated 236,100,000 ransomware attacks around the globe.
Source Link

- **Intellectual Property and Regulated Data Loss**: After an attacker successfully executes their attack, they don't simply deny access to your data – they will send that data outside of your network and threaten to leak it publicly. For many organizations this exposure of customer data has regulatory implications and can lead to lawsuits and fines. Additionally, sensitive data on corporate transactions, patents, etc. can end up in the attackers' hands and be sold to the highest bidder on dark web forums.
- **Incident Response and Remediation Costs:** The average incident response cost for a ransomware attack is $4.54 million, more than the average cost of a data breach at $4.35 million. While larger organizations can absorb these costs, this potentially represents an existential threat to smaller companies.
- **Associated Costs to the Business:** The above figures did not even include the ransom payment, the long-term damage to an organizations' brand (loss of consumer trust), increased cyber insurance premiums, legal fees, or lost revenue which can far exceed remediation costs – this is why the focus needs to be on both prevention and resilience.

For a wider variety of organizations this exposure of customer data has regulatory implications which can also lead to lawsuits and fines.

The average ransomware attack incident response costs $4,540,000 more than the average cost of a data breach at $4,350,000.

Small businesses saw a 40% increase in ransomware attacks.

The average downtime for companies hit by ransomware is 7-12 days.

02 RaaS and the Ransomware Economy

The rise of Ransomware as a Service (RaaS) gangs mimics the more conventional Software as a Service business model in every meaningful measure. **The ransomware economy involves multiple players who specialize in various aspects of the larger ransomware attack.** These elements include:

- **Initial Access Brokers:** Initial Access Brokers (IABs) are highly skilled specialists who are exceptionally good at penetrating and establishing a foothold within secure networks. IABs often sell access to these compromised networks to other threat actors, including ransomware affiliates. The deeper an IAB can penetrate a network, the more valuable their services become. Purchasing credentials and access is surprisingly easy and relatively inexpensive.
- **RaaS Platform Providers:** Ransomware-as-a-Service (RaaS) operators provide the software platform and backend to launch attacks. They have development teams constantly improving their feature sets, they assist in negotiations during a successful attack, they manage customer service agents, market to new affiliates, and more all for a slice of the profits.
- **RaaS Affiliates:** The actual ransomware attack is managed and executed by an affiliate; a person or group who plans and carries out the attack campaign. They obtain access via an IAB (or create their own), use a platform or toolkit from a RaaS operator, execute the attack, and then move the ransom dollars around to stay below the radar.
- **Crypto Exchange Money Launderers:** The money launderers do just that – move illicit ransom payments through crypto exchanges with the intent to hide both the origins and the destination of the funds and then take a healthy fee for their services.

The overall maturity, level of organization, and specialization within the ransomware economy means **we are dealing with an adversary whose tactics, techniques, and procedures (TTPs) are approaching the sophistication of some nation-state-sponsored attackers.**

In many cases, there has been documented overlap between nation-state attack elements and those of cybercriminal ransomware gangs. Today's ransomware attacks are more complex and difficult to defend against than ever before.

Stages of a Ransomware Attack

These more complex, multi-stage ransomware attacks typically follow the same attack progression, with some variance depending on the attack group and the selected target. The four stages of a ransomware attack generally include:

STAGE 1: INITIAL INFECTION, PERSISTENCE, AND COMMAND AND CONTROL

Traditionally, initial infections include malicious attachments or links to malicious websites delivered via phishing emails or drive-by attacks, or through stolen or brute-forcing user credentials.

> **More advanced ransomware operators are increasingly leveraging automation to identify exposed organizations that have not patched against known vulnerabilities and have compromised APIs.**

STAGE 2: PRIVILEGE ESCALATION AND LATERAL MOVEMENT

Once inside, ransomware operators seek to move laterally and vertically through the network to **get access to as much of the environment as possible, locating sensitive data to exfiltrate and compromising more users and systems before detonating the ransomware payload.** Key to this progression is the escalation of user privileges through social engineering, credential theft, or the exploitation of vulnerabilities and misconfigurations in operating systems and applications.

Other techniques commonly used are privilege escalation, and lateral movement including brute-forcing weak passwords, credential spraying/stuffing techniques, and outright credential dumping where the attack has gained access to multiple credential sets. At the end of this stage, the attacker typically has all the privileges of a network administrator.

STAGE 3: DATA EXFILTRATION

Data exfiltration occurs when a threat actor engages in an unauthorized data transfer from a computer, server, or other network system without the consent of the system's owner. The types of data threat actors exfiltrate typically include the personally identifiable information of clients or employees, information related to payment processing, the organization's business dealings, trade secrets, and intellectual property, and other data the attacker can leverage for tactical or financial gain.

Specific to ransomware attacks, threat actors have increasingly engaged in data exfiltration prior to the detonation of the ransomware payload that encrypts the targeted systems.

> **Ransomware operators may use exfiltrated data in Double Extortion schemes to compel the target to pay the ransom demand under the threat that the data will be exposed if payment is not received by a deadline set by the attackers. More on the implications of this trend in the next section.**

STAGE 4: PAYLOAD DETONATION AND EXTORTION

Delivery of the ransomware payload initiates the file encryption process that can render data, devices, and systems inaccessible, and usually includes delivery of a message or ransom note that informs the system owners of the attack and provides instructions on what they should do next about meeting the attacker demands to regain access. This typically involves the payment of a ransom demand and marks the beginning of the extortion process.

Ransomware attacks, as well as direct data extortion attacks that do not involve a ransomware payload, are somewhat unique in that the threat actor intends to reveal the attack to the victim, unlike other attacks that seek to remain undetected while the intruder continues to harvest and exfiltrate sensitive data.

The focus of most discussions around ransomware is on this stage of the attack, despite the ransomware payload being delivered near the end of the attack sequence. **In today's more complex ransomware attacks that include data exfiltration, there are weeks or even months of detectable activity occurring on the network** as described above.

At this point, the attacker has all but succeeded in the attack. Whether or not the organization **pays a ransom demand or chooses to remediate without cooperating with the attackers, the organization has already been disrupted, and for the most part, the damage has already been incurred.**

This is why it is important for organizations to develop a ransomware defense strategy that focuses on both preventions – stopping the attack before the ransomware payload is delivered – as well as emphasizing resilience – what it will take to ensure that operations are returned to normal swiftly with as little disruption to the organization as possible.

Spotlight: Data Exfiltration

Data exfiltration and the threat of exposure are now a central aspect of nearly every ransomware operator's playbook and significantly increase the chances for the extortion efforts to be successful.

The Double Extortion tactic begins when they exfiltrate sensitive information from the target before launching the encryption routine. The threat actor then makes the additional demand that victims pay up to prevent the attackers from publishing their data online.

We see this most clearly in the evolution of the extortion tactics employed by the ransomware actors. Originally, the malicious payloads would encrypt files and demand payment for decryption keys. Security teams found success in either restoring from backups or accepting loss of data as an acceptable consequence.

Cybercriminals evolved and introduced data exfiltration capabilities into their attacks, where they not only demand payment of a ransom to regain access to encrypted systems, but they also demand further payment for the stolen data itself. Of course, there is no guarantee that payment will protect the stolen data from being exploited.

03 Top Ransomware Infection Pathways

Ransomware operators and other threat actors employ a wide variety of attack vectors to infiltrate a target network. Here are a few of the most common infection pathways:

PHISHING AND OTHER SOCIAL ENGINEERING ATTACKS

Social engineering attacks are the most common way ransomware operators get initial access to a targeted network. Phishing via malicious emails or messages on social platforms is a favorite tactic. Specially crafted emails are designed to trick targets into clicking malicious links, opening tainted attachments, or providing sensitive information like user credentials. Attackers who have already successfully infiltrated a network may also use social engineering techniques to compromise identities that have more user privileges at a targeted organization, like network admins and company executives.

> **More than 50% of ransomware victims indicated that phishing was the initial infection vector***

UNSECURED OR COMPROMISED RDP AND VPN CONNECTIONS

Abusing Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) are some of the more common tactics used by ransomware operators to move laterally and vertically in a compromised network. RDP exploits are also used to remotely execute malicious code like malware and attack kits, or by executing scripts in fileless attacks, or when abusing legitimate network tools in what is known as living-off-the-land. Access to RDP and VPN instances is usually accomplished by way of stolen or brute-forced user credentials.

WATERING HOLES, MALICIOUS AD LIBRARIES, DRIVE-BY ATTACKS

Many forms of malware, including ransomware, are distributed through other social engineering attacks. Watering hole attacks include legitimate websites (or fake sites that look to be legitimate) likely of interest to a targeted audience that have been compromised to serve up malicious code. Attackers also compromise ad libraries to use in propagating ransomware in drive-by attacks where the victim can be infected simply by visiting a legitimate website that is pulling in the compromised advertisements for display.

COMPROMISED SOFTWARE DOWNLOADS

As we saw in the case of the Kaseya supply chain attacks, victims can be compromised by a legitimate software update from a known vendor that was signed with a valid digital certificate. Kaseya is a managed services provider, and their remote management service was exploited by the REvil ransomware gang which in turn compromised customers around the world. REvil exploited a known vulnerability that Kaseya was just in the process of validating for a patch. Even the best security hygiene efforts cannot prevent this kind of attack from being successful.

ZERO-DAY AND UNPATCHED VULNERABILITY EXPLOITS

Patching systems can be a complex process for some organizations. In order to avoid breaking critical business systems, patches often need to be applied in dev environments and tested prior to being put into production. Even then, some issues prevent patching due to legacy systems/software or internal (home-brewed) scripts/applications that will break if the patch is applied haphazardly. Thus, there can be months or more of work to do before some vulnerabilities can be mitigated, leaving the organization exposed.

BRUTE-FORCED AND STOLEN AUTHENTICATION CREDENTIALS

As mentioned above, attackers are keen to get their hands of stolen user credentials and often use social engineering techniques to obtain them, or they can also look to the dark web marketplaces for user credential other threat actors are offering for sale. Attackers also benefit from reused credential that have been compromised at other sites or use brute-force and dictionary attacks where they automate credential "guessing" at high volumes.

UNHOOKING AND BYPASSING ENDPOINT SECURITY TOOLS

Ransomware attackers are adept at bypassing security controls, and endpoint protection tools are no exception. There are numerous examples of hard-coded AV/NGAV/EDR/XDR bypasses written into malicious code that lets the attack slip by without an alert being triggered. Attackers have also been observed using "universal unhooking" to bypass security tools. Code hooking is a technique used by legitimate software, including endpoint protection tools, to gain needed visibility into activity on the network.

> **Universal unhooking techniques hijack execution flow and allow attackers to deploy a rootkit, for example, then obfuscate subsequent processes and network connections. Universal unhooking basically blinds endpoint protection tools to the malicious activity, rendering them ineffective for detecting the attack.**

NETWORK, SYSTEM AND SOFTWARE MISCONFIGURATIONS

A misconfiguration is the improper deployment or tuning of software deployed in a network that leaves the tool and/or the network vulnerable to attack. Orchestrating all the components of a large network (or even a small one) is an art form and requires a great deal of skill. Minor errors in configurations can leave application instances and even the entire network exposed.

ATTACK TOOLKITS AND ABUSING LEGITIMATE NETWORK TOOLS

Attackers often use legitimate penetration testing tools – like Cobalt Strike and Mimikatz, for example – to compromise a network, to move laterally or vertically, to steal user credentials and more. Attackers also abuse legitimate tools that are already on the network – like PowerShell and PsExec – for malicious activities.

> **The use of legitimate tools reduces the likelihood the attackers will be discovered and negates the need for them to develop additional tooling for an attack.**

Recovering from a ransomware attack is generally 10X the amount of the ransom payment request. Source Link

The world's largest meat supplier JBS was forced to suspend operations for 11 days despite paying an $11,000,000 ransom demand. Source Link

04 Defending Against Ransomware Attacks

The attacks targeting organizations for large ransom payouts today are complex multi-stage operations, and the ransomware payload is typically at the tail-end of the longer attack sequence.

This means **there are typically weeks or even months of detectable activity on the network that occurs before the data and systems are rendered inaccessible** and a ransom demand is issued. A robust ransomware defense begins with assuring the organization has the basics down.

The following are controls and procedures every organization should implement even when not taking the threat of a ransomware attack into consideration to establish a baseline security posture:

- **Patch Management:** Keep all software and operating systems up to date and patched.
- **Data Backups:** Assure critical data is backed up off-site and protected from corruption in the case of a ransomware attack.

> **95% of ransomware attacks also attempted to infect backup repositories**

- **Access Control:** Implement network segmentation and policies of least privilege (Zero Trust).
- **Awareness:** Implement an employee awareness program to educate against risky behaviors, phishing techniques, etc.
- **Procedure Testing:** Plan and prepare for failure by running regular tabletop exercises and ensuring all stakeholders are ready and available to respond to an attack at all times.
- **Resilience Testing:** Regularly test solutions against simulated ransomware attacks to assure effective detection, prevention, response, and full recovery of targeted systems.

Basic security hygiene is not enough though. **Most attacks start at the endpoint, so endpoint security and resiliency are essential.** Let's take a deeper look at the evolution of endpoint protection, the tools available, and where they fall short in defending against ransomware attacks.

Endpoint Security

The concept of endpoint security is simple: protect endpoints like servers and end-user devices like desktops, laptops, tablets, mobile devices, and more from unauthorized access and exploitation. The practice of defending endpoints effectively? That is far from easy.

The security industry continues to evolve means and methods for improving endpoint security – here is a rundown of the last 40 years of endpoint security product evolution:

FIREWALLS

The most basic is a software-based firewall software for endpoint devices, which is designed to regulate traffic to the endpoint it is installed on and prevent malicious interactions and some unauthorized installations. But firewalls, while important, are easy to bypass and have limited utility, so in addition, organizations deploy a traditional (AV) or next-generation antivirus (NGAV) is highly recommended.

TRADITIONAL ANTIVIRUS

If kept up-to-date and continuously running, traditional signature-based AV will protect an endpoint from infection by most known malware families. The problem is that they are simply unable to detect and block novel or altered versions – such as if the malware has been repacked – until a human manually writes a new detection signature is created and pushed out to the endpoints in the form of an update.

> **Traditional AV requires a lot of resource consumption on the endpoint as new signatures are downloaded and the device is rescanned daily**

AV is also extremely resource heavy – not just to produce new signatures and keep devices up to date, it also requires a lot of resource consumption on the endpoint as new signatures are downloaded and the device is rescanned daily. Scans are time consuming because they essentially have to look for every single piece of malware every single time. Realistically that's not possible, so they stop looking for older malware versions, attackers often resurrect them, and AV misses the detection. This is where NGAV comes into play.

NEXTGEN ANTIVIRUS

NGAV solutions usually employ Artificial Intelligence (AI) machine learning (ML) for detections based on the pre-execution characteristics of the code. This means they do a decent job of recognizing and blocking novel and altered malware strains that traditional AV misses and new detections are not constrained by the manual process of signature development.

NGAV has its limitations, often missing some unique malware variants and producing a high volume of false positives. The inability to prevent 100% of malware – in addition to the introduction of living-off-the-land, fileless, and other advanced attack techniques – prompted the advent of Endpoint Detection and Response (EDR) and its more comprehensive cousin Extended Detection and Response (XDR).

ENDPOINT DETECTION AND RESPONSE

EDR delivered the ability to leverage AI/ML algorithms to analyze behaviors on the network to identify malicious operations in progress. It also enabled security teams to proactively threat hunt in their environments for the more subtle indicators of compromise that can expose an attack at subsequent stages. EDR changed the entire security landscape for the better, but it also has its limitations.

> **First, the AI/ML models are tremendously complex and take years to train, and the detections are only as good as the samples they were trained on.**

Also, EDR only provides acute visibility into what is happening on the endpoint, with limited visibility of the other network components aside from how they interact with those devices.

EXTENDED DETECTION AND RESPONSE

XDR solutions on the other hand, were designed as a logical extension of EDR with the benefit of correlating behavioral telemetry from other parts of the network. In this way, security teams can see not just what is happening on the endpoint, but also how that behavior is possibly related to user identity and authentication, or assets in the cloud, and across the entire IT and security stack.

> **XDR, while promising, still suffers from the same issues as other EPP tools: they are susceptible to bypassing and unhooking, they are difficult to configure and manage properly, and they usually have a high false positive rate – all of which means additional strain on already maxed-out security teams.**

They also are dependent on complex AI/ML behavior detection models that take years to create, so they are not very agile when it comes to updating them as threat actor TTPs evolve. It is a tremendous lift to introduce a new model into production in client environments, and a small flaw in the training data for the model can mean big problems for its efficacy.

Baltimore City Ransomware Attack Will Cost More Than $18,000,000

The city of Baltimore was crippled for over a month, and estimates that the May 7 ransomware attack on city computers will cost at least $18.2 million to restore systems and make up for lost or delayed revenue. Source Link

Why So Many Successful Ransomware Attacks?

It is more than apparent with new victims and higher ransom demands in the headlines daily that traditional endpoint solutions – while essential to any security program – are simply not designed to detect and stop ransomware attacks.

If they could, they would. But they can't, so they don't.

This is why Halcyon 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 works.

05 The Halcyon Anti-Ransomware and Cyber Resilience Platform

Organizations that are concerned about the threat of a successful ransomware attack need a solution that is purpose-built and specially crafted to detect and defeat the most advanced ransomware operations. This is where Halcyon enters the equation and provides organizations with an edge against this rapidly evolving threat.

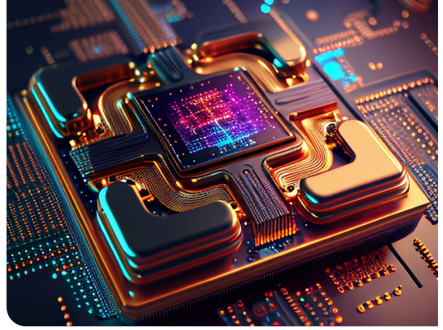
The Halcyon Anti-Ransomware and Cyber Resilience Platform is a lightweight agent that combines multiple proprietary detection, prevention, and response engines powered by advanced AI/ML decision models that were trained solely on ransomware samples, making them far more efficient and effective than models trained to look for more common forms of malware.

The Halcyon Anti-Ransomware and Cyber Resilience Platform detection engines were trained to primarily detect ransomware. This gives them a distinct advantage over NGAV/EDR/XDR AI/ML models.

The Halcyon Difference

Other AI/ML endpoint protection models were trained on characteristics that all malware share, including some ransomware samples in the mix. But ransomware does not behave like other malware, so training AI/ML models on the few characteristics that ransomware does share with other malware leaves a lot of room for missed detections.

Conversely, the Halcyon AI/ML models were trained on characteristics that all ransomware share to deliver more efficient and effective detection of ransomware attacks. Halcyon also uses multiple proprietary AI/ML micro-models that work together for ransomware pre-execution and behavioral detections.



> **This means that as new features are introduced by ransomware operators or gaps in coverage are discovered in existing models new AI/ML micro-models can quickly be trained and deployed with zero interruption to users, systems, or the network.**

Additionally, the Halcyon solution is designed to be deployed alongside other EPP solutions, protecting them from attacks and enhancing their detections. What really sets Halcyon apart from other solutions is **the protective kernel architecture of the platform: Halcyon protects other endpoint security tools that are running in tandem from being blinded, unhooked, or uninstalled by attackers.** The Halcyon Anti-Ransomware and Cyber Resilience Platform also amplifies bad behaviors to bolster detections by other endpoint tools, making them more effective. If no endpoint security solution is active, Halcyon will enable Windows Defender (and other select products) and ensure it is up to date.

The Halcyon Advantage

The *Halcyon Anti-Ransomware and Cyber Resilience Platform* is the first and only contextually aware, purpose-built ransomware prevention solution that hardens endpoints against how ransomware specifically works.

Halcyon autonomously isolates the impacted device to protect the larger network, neutralizes the attack in progress, captures the encryption key, and decrypts the impacted device, enabling organizations to recover quickly from an attack. The Halcyon Anti-Ransomware and Cyber Resilience Platform delivers:

LAYER 01: PRE-EXECUTION RANSOMWARE PREVENTION

Our pre-execution layer leverages multiple external threat intelligence feeds, proprietary Halcyon threat intelligence and through AI/ML analysis to deliver an instant response for any "known bad" binaries. Suspicious executables that are not "known bad" are then passed to the additional protection layers for further analysis.

LAYER 02: EXPLOITATION OF RANSOMWARE FEATURES

Ransomware operates within the confines of a ruleset to prevent it from being detected and to shield the operators from attribution.

> **The *Halcyon Anti-Ransomware and Cyber Resilience Platform* tricks ransomware into aborting the attack or revealing itself by exploiting features hardcoded in the ransomware.**

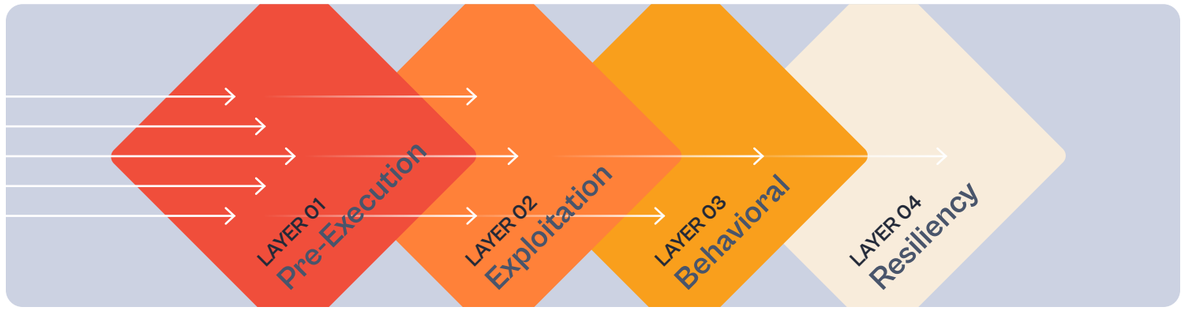
The Halcyon Exploitation layer triggers this ruleset via deception techniques to prevent detonation or amplify bad behavior. This protection layer enables the endpoint to exploit anti-analysis routines, laces the endpoint with artifacts to deceive the ransomware's internal execution rules, and adds "bait files" or injects artificial services into the view of the process to amplify the ability to detect malicious behavior.

LAYER 03: ADVANCED RANSOMWARE BEHAVIOR DETECTIONS

Advanced and novel forms of ransomware are designed to circumvent pre-execution tools like AV/NGAV and can detect when they are in controlled environments used for analysis, rendering those tools ineffective. Ransomware variants that can circumvent Layers 01 and 02 will trigger the protection offered by Halcyon's third layer due to its own deconfliction check attempts or in the process of initiating its core functions.

LAYER 04: ENDPOINT AND NETWORK RESILIENCY

Halcyon is the first endpoint cybersecurity product to automate resiliency and isolation capabilities to mitigate the overall impact of a ransomware event even if all other protection layers fail. Our multiple layers of protection are further backed by several levels of endpoint resiliency specifically designed to prevent a ransomware infection from spreading to other endpoints, reducing the potential impact of a successful ransomware attack.



The Halcyon Mission: Defeat Ransomware

Legacy security tools were simply not designed to address the unique threat that ransomware presents, so we keep seeing destructive ransomware attacks circumvent these solutions. *The Halcyon Anti-Ransomware and Cyber Resilience Platform:*

- Detects and blocks both known and novel ransomware families via multi-layer, AI-powered prevention, detection and response engines.
- Delivers built-in endpoint agent hardening and ensures existing solutions are protected from bypass and unhooking techniques.
- Provides redundant resiliency features through autonomous host isolation and encryption key capture for swift automated recovery.

The unique *Halcyon Anti-Ransomware and Resilience Platform* is easy to deploy, does not conflict with existing endpoint security solutions, and provides multiple, unique levels of protection against ransomware attacks. Halcyon is the first platform to leverage advanced AI/ML detection models specifically trained to defeat ransomware.

Talk to a Halcyon expert today to find out more and take a look at our resource site, Recent Ransomware Attacks to get near real-time tracking of ransomware attacks, threat actor groups and their victims.

Ready to Chat? Contact Us

Modern defensive cyber solutions, while impressive, have failed in the face of cheap and easy-to-create – and most importantly lucrative – ransomware. High-profile breaches are disguising an ugly fact; the companies using next-generation EPP, EDR and XDR solutions continue to be impacted by ransomware.

Halcyon is the world's first cyber resilience platform designed from day one to defeat ransomware. Global 2000 companies rely on Halcyon to augment existing EPP, EDR and XDR platforms and undo attacks in minutes with bypass and evasion protection, key capture and automated decryption, as well as exfiltration and extortion prevention. For more information, visit https://www.halcyon.ai/

Interested in getting a demo? Let's talk.

sales@halcyon.ai
855-8-HALCYON

halcyon