halcyon

Technical Deep Dive: What is Cyber Resilience?

How Halcyon Defines Cyber Resilience

From the proto-viruses of the 1970s like Creeper to full-blown cyber weapons like Stuxnet and the rise of nation-state Advanced Persistent Threat (APT) groups, the history of malware has continued to evolve from the moment computers were first networked together. For most of this history, viruses, and malware were used for experimentation, hacktivism, denial of resources, and espionage but as digital currencies like Bitcoin took off, so did the ultimate form of cybercrime: ransomware.

Ransomware is not new, it's been splashed across the headlines of many news publications over the years. From NotPetya to LockBit and Conti, the cybersecurity industry has had to face a new and more motivated attacker leveraging advanced techniques, leaks of intelligence assets, and a persistent desire to extract money from victims.

Security tools like Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) rapidly had to shift from stopping commodity malware to defending against a new threat that could bring a victim organization down for days and weeks. Ransomware, unfortunately, is winning with 236,100,000 ransomware attacks globally in the first half of 2022.

Cybersecurity goes through continual cycles of innovation and stagnation and ransomware attackers know this well. Of the top 20 most actively tracked ransomware groups, the majority leverage bypasses and evasions to get around cybersecurity tools after they've gained entry to a network through an Initial Access Broker (IAB). **Since ransomware can effectively stop a business from operating, as seen in the 2021 attack on Colonial Pipeline, it's time for a new way to approach building cybersecurity programs.**

Building A Resilient Enterprise

PEOPLE AND PROCESS

Historically users have always borne the brunt of the blame as the entry point for a cyberattack. While true, most access involved phishing, social engineering, or an errant click on a document, it's time for security providers to stop blaming users and build better products. Whether user education or untested remote backup procedures, people and processes will fail. A resilient enterprise does not rely on any single point of failure and always assumes compromise.

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.

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

PROACTIVE PRODUCTS

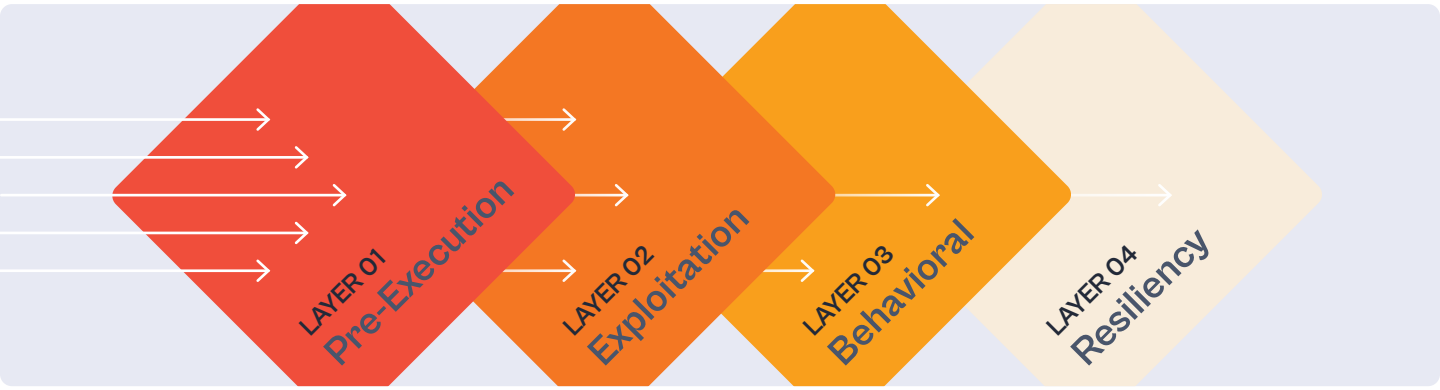
Many security products are effective for a time, but as they become popular, attackers shift their attention to bypassing and reverse engineering detection methods. A resilient enterprise incorporates products with modular and expandable architectures that quickly adapt to new threats. Companies with legacy technical debt typically must acquire other technologies and haphazardly integrate them into their core products to extend feature sets.

DEFENSIVE RESILIENCE

Cybersecurity is a team sport where “better together” trumps “best of breed.” Resilient organizations adopt products that augment, support, and armor other security tools instead of conflicting with them. All security agents on an endpoint are a target for an attacker and products that help with protecting these tools ensure that the business will stay operational despite a breach.

OPERATIONAL RESILIENCE

Every minute that a crucial system is down has a real impact on the business. Whether it's a server hosting internal file shares or the laptop of an employee in accounting, there is a dollar cost to each system that is down. With enough systems down, the business may fail. Recovery time from a ransomware attack is estimated to be between 7 and 21 days, far too long to be acceptable. Resilient products leverage automated recovery of encryption keys, instant decryption of endpoints, and ways to armor and protect system backups from being impacted by an attack.



Halcyon Anti-Ransomware and Cyber Resilience Platform

Halcyon was designed as the first product to leverage a resiliency framework in the fight against ransomware. With 236,100,000 global ransomware attacks in the first half of 2022, it's clear that the existing story of stand-alone products in a security stack is not working. For a limited time Halcyon is offering a Ransomware Readiness Report available to all organizations above 2,500 endpoints to show what a resilient approach to ransomware looks like.

For more information 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 ransomware readiness report today!