halcyon

Data Sheet

Cyber Resilience for the Post-Mythos Era

Mythos Didn't Create the Vulnerability Gap. It Proved How Big It Really Is.

AI hands attackers more firepower, but not a new playbook: they're still running the same exfiltrate, encrypt, extort sequence that's always worked, just faster now. Self-healing patch management still doesn't exist. Even the roughly 200 organizations already inside Anthropic's Project Glasswing (some of the best-resourced security teams anywhere) are finding new vulnerabilities about five times faster than they can patch them. Large enterprises can face hundreds of thousands of low-priority findings in every patch cycle. Worse, attackers don't need to exploit every vulnerability. They only need to chain together a handful of overlooked weaknesses to gain an initial foothold. AI simply makes it easier to find those chains.

This is the gap Mythos actually revealed. The breakthrough wasn't AI discovering vulnerabilities. It was proof that discovery has permanently outpaced remediation. Even the world's best-funded security teams cannot patch as fast as modern AI can uncover weaknesses. Traditional prevention was never designed for this new reality.

Why the Post-Mythos Era Demands Resilience, Not Just Prevention.

THE PATCH RACE IS STRUCTURALLY UNWINNABLE

Even the best-resourced Glasswing organizations find vulnerabilities faster than they can close them. A known, unpatched vulnerability is often the more dangerous one: attackers weaponize it faster than defenders can remediate.

RANSOMWARE OPERATES LIKE A BUSINESS

Modern groups run negotiation teams, PR outreach, and access brokers on business hours. Same tools as a red team, with more time, more motivation, and no rules of engagement. Prevention was never built to stop a patient human intruder who already has access.

CYBER RESILIENCE HAS ALWAYS MEANT BUSINESS RECOVERY

Business recovery, not cyber recovery. Most programs answer "how do we keep running after an attack," not "what do we do the moment defenses fail." That gap leaves a playbook and a call to the insurer instead of a real capability.

ATTACKERS TARGET THIRD PARTIES ON PURPOSE

Attackers go after organizations with the largest vendor networks on purpose, because supply-chain pressure translates directly into ransom leverage. Undocumented dependency maps and untested disconnect/reconnect plans turn that exposure into leverage attackers can count on.

Post-Mythos Era: Why Halcyon?

Prevention plus resilience means having a plan for the moment prevention fails, not just for the exploit that got an attacker in. That's the point of assuming breach: with AI giving attackers more firepower and machine speed on their side, Halcyon builds layers of resilience rather than betting everything on keeping them out. It provides that "right of boom" capability, at the speed the threat now moves:

- **Right-of-Boom Response:** Evicition-as-a-Service detects, contains, and removes a ransomware attacker in minutes, not weeks.
- **Backup Tamper Protection:** Blocks attempts to disable, encrypt, or corrupt backup infrastructure before recovery options disappear.
- **File Resilience:** Detects encryption in progress, stops it, and reverses malicious changes in real time.
- **Encrypted File Recovery:** Captures key material to decrypt impacted files without backups, cutting recovery from weeks to minutes.
- **Data Exfil Protection (DXP):** Stops data theft before it leaves the environment, a gap no patch cycle or scanner closes.
- **Ransomware Operations Center (ROC):** Ransomware experts are on call 24/7 to detect, contain, and recover in minutes, at no extra cost.

Halcyon vs. Traditional Prevention: Resilience for the Post-Mythos Era

CAPABILITY	TRADITIONAL PREVENTION	HALCYON
Patch-Race Assumption	Assumes you can close a vulnerability before it's exploited, an assumption that breaks down when discovery outpaces patching roughly 5-to-1, even for the best-resourced teams inside Project Glasswing.	Halcyon assumes breach. Instead of waiting on the patch cycle, it's built to contain the attack and evict the attacker before they can cause business disruption, watching for compromise behavior on the assets that matter most while remediation plays out.
Resilience Philosophy	Treats resilience as business recovery, restoring operations after the fact, while the cyber failure itself goes unaddressed.	Halcyon treats resilience as keeping the business running through an attack, not recovering it quickly after the fact. It contains and isolates the threat in the moment, so operations continue instead of going down first and racing to restore later.
Attacker Profile	Focused on stopping known exploits and vulnerabilities, not the human-led, business-like campaign that follows once an attacker is already inside.	Halcyon is built for that adversary specifically, detecting the behaviors ransomware operators rely on, not signatures they've already learned to evade.
Third-Party Blast Radius	Protects your own systems only. Does nothing when a vendor you depend on is compromised, or when your own downtime becomes their liability.	Halcyon contains the blast radius inside your own environment, so a compromise on either side of that relationship doesn't turn into extended downtime or a wider attack path.
Recovery Speed	Traditional recovery often means restoring entire systems from backup, a process measured in days or weeks.	Halcyon contains attacks early and minimizes the blast radius, so recovery never means rebuilding the whole environment. If encryption gets through, captured key material recovers the data without backups.
Managed Response	Incident response against a fast-moving, human-led campaign requires a separate engagement, often too slow to matter.	The 24/7 Halcyon ROC delivers eviction-as-a-service style response, at no additional cost.

Insights drawn from Halcyon's Mythos or Reality: How AI Changes Ransomware Resiliency panel discussion.

Prevention Isn't the Whole Strategy

AI changes how quickly and how often attackers get in, and breach should be assumed. What matters is whether the attacker can be detected, contained, and evicted before the business feels it. Halcyon is built for that window, containing the attack in progress, minimizing the blast radius before it spreads, and keeping the business running instead of depending on a full recovery to bring it back.

The result is less data lost, fewer systems requiring full restoration, and recovery measured in minutes rather than weeks, no matter how the attack got in.

The Post-Mythos Reality

In the post-Mythos era, vulnerability discovery is accelerating faster than organizations can remediate. Attackers need less expertise to gain initial access, while ransomware operations continue to professionalize. That changes the economics of defense. Prevention remains critical, but organizations also need the ability to contain, recover, and continue operating after compromise. That's the resilience gap Halcyon is designed to close.

Halcyon is built for this new reality. To see how Halcyon can improve your cyber resilience and maintain business operations through a ransomware attack, reach out to request a demo. Learn more at www.halcyon.ai.