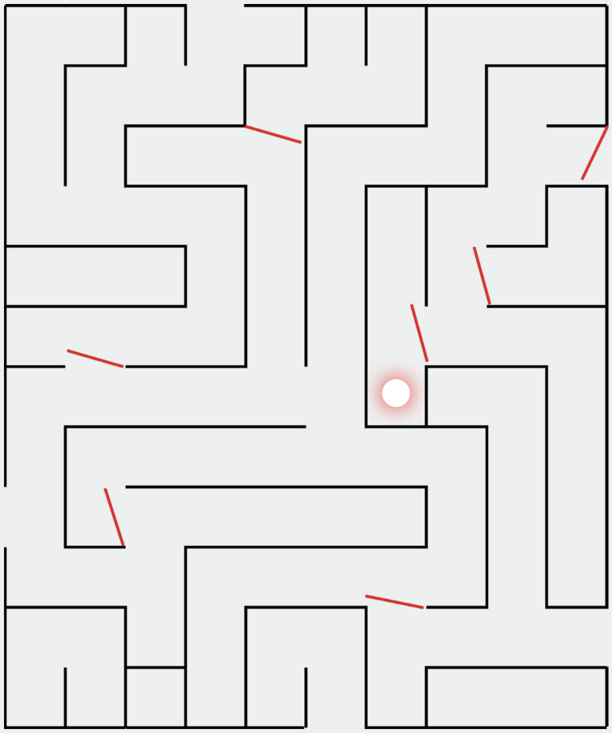
ARMS CYBER

# Ransomware Resilience REIMAGINED

**A Three-Phase Strategy to Stop Attacks Before, During, and After Execution**

## Introduction

Ransomware has evolved beyond traditional defenses. With AI-driven automation, Ransomware-as-a-Service (RaaS), and stealthy fileless techniques, attackers now move faster and smarter than ever. Signature-based detection and reactive response strategies can't keep up.



## Arms Cyber changes the game.

Built on a patented three-phase model—**Preempt, Block, & Remediate**—the Arms platform prevents attack damage before it starts, detects and neutralizes active threats in real-time, and restores operations in minutes.

It works alongside existing tools like EDR, XDR, and SIEM to close critical gaps—especially around memory-based and fileless ransomware.

## Preempt:

### Protection from Ransomware Before It Starts

The first phase is about proactively hardening against ransomware before execution. Arms Cyber shrinks the attack surface and blinds adversaries through stealth and diversity. These proactive defenses make the system unpredictable and unrewarding for attackers, forcing them to fail early and move on to the next target.

- **PowerShell Protection** stops obfuscated and malicious commands before they run, blocking a key vector for fileless attacks and malware droppers.
- **Stealth Directories** hide critical files and assets from view—if ransomware can't find them, it can't encrypt or steal them.

## Block:

### Detecting and Stopping Attacks in Real-Time

If a threat gets through, Arms Cyber activates real-time behavioral defenses—without relying on static signatures. This phase neutralizes active attacks with speed and precision, reinforcing traditional EDR/XDR platforms and catching what they miss.

- **Stealth Decoys** lure ransomware into interacting with fake files, triggering detection safely and silently upstream before encryption has the chance to expand.
- **File Entropy Analysis** detects early encryption behavior by monitoring changes in the file data entropy.
- **Encryption Mitigation** halts unauthorized encryption attempts mid-process—even from unknown variants.

## Remediate:

### Rapid Recovery with Minimal Downtime

Even when ransomware compromises a system, Arms Cyber ensures operations resume in minutes—not days. With average downtime costing thousands per minute, Arms Cyber cuts potential losses by millions and prevents ransom payments altogether.

- **Stealth Vault** continuously saves secure file versions in hidden enclaves, immune to discovery or tampering.
- **Rapid Remediation** instantly restores files from these clean versions without user action or backup delays.

## Conclusion

Arms Cyber delivers true ransomware resilience. Through **preemptive stealth posture management**, **real-time behavioral defense**, and **instant recovery**, it renders ransomware ineffective—before, during, and after an attack.

**In a threat landscape where speed and adaptability define the winners, Arms Cyber ensures you stay ahead.**