halcyon

Data Sheet

Halcyon Greenlight Service: Immediate Containment, Lasting Security

Rapid Containment. Secure Recovery. Lasting Protection.

Ransomware attacks throw organizations into immediate firefighting mode, focusing all efforts on stopping the attack and initiating recovery. Attackers anticipate this chaos and often use it as cover to create backdoors, lay traps for future attacks, and ensure they can re-enter the environment undetected. While standard incident response teams are effective at broad cyber recovery, they often lack the specialized ransomware expertise needed to detect and eliminate persistent threats left behind. Halcyon Greenlight was created to close this critical gap, ensuring recovery, true attacker eviction, and environment lockdown.

An Overview of Halcyon Greenlight Service

Halcyon Greenlight delivers rapid deployment of Halcyon's anti-ransomware technology and elite incident response teams to contain cyber threats immediately post-incident. Greenlight secures your environment to prevent attackers' re-entry and ensures safe, accelerated recovery.

How Is Halcyon Greenlight Different?

- **$0 Technology Cost During IR:** Deploy Halcyon and leading EDR and forensic technologies at no cost during the active incident.
- **Dual Visibility:** Inside-out (internal environment) and outside-in (external attack surface) threat detection from day one.
- **Complete Backup Lockdown:** We don't just recommend secure backups – we implement them immediately.
- **Legal Counsel Alignment:** Integration with internal and external legal teams as part of the standard process.
- **Specialized Ransomware Focus:** Explicitly designed to neutralize ransomware and disruptive attacks.

Our Expert-Led Team

- Led by elite specialists with prior experience at **Mandiant**, **Accuvant**, and **Kivu**.
- Embedded Incident Commander to provide technical counsel and executive communication.

Halcyon Features

- Always Included 24/7/365 Expert Threat Monitoring and Recovery
- Pre-execution Prevention
- Ransomware Behavior Detection
- Encryption Key Material Intercept
- Data Exfiltration Protection

About Halcyon

Halcyon is the only cybersecurity company that eliminates the business impact of ransomware. Modern enterprises rely on Halcyon to prevent ransomware attacks, eradicating cybercriminals' ability to encrypt systems, steal data, and extort companies. Backed by an industry-leading warranty, the Halcyon Anti-Ransomware Platform drastically reduces downtime, enabling organizations to quickly and easily recover from attacks without paying ransoms or relying on backups.

Greenlight Rapid Response Model

Ransomware

- An attack and/or payload is successfully executed.
- Ransom note and extortion demand made.

Team Activation

- IR team deployed immediately with Halcyon, EDR, and Forensic technology stack.
- Alignment with legal counsel and leadership.

Threat Visibility

- Internal telemetry and forensics initiated.
- External attack surface monitoring launched

Environment Locked

- Backup isolation and protection implemented.
- MFA hardened across enterprise.
- Public-facing infrastructure secured.
- Identity access audited and de-provisioned.

Executive Reporting

- High-level exec summary and in-depth technical reports provided.
- Hardening and recovery roadmaps recommended.
- Transition hand off.

Executive-Ready Deliverables

- Tailored executive briefings for leadership and board-level stakeholders.
- Detailed technical findings and prioritized remediation recommendations.

What You Walk Away With:

- Contained and locked-down environment ready for recovery.
- Verified, secured, and isolated backups.
- Executive-level incident briefing and detailed technical assessment.
- Prioritized action plan for immediate and mid-term security improvements.

Ready to Get Started?

Protect your organization from ransomware threats with Halcyon Greenlight, the service that kicks the bad guys out – and keeps them out.

Immediate Response Available 24/7 via Halcyon Emergency Response Team
Phone: +1 (210) 830-9940

100% of organizations were prevented from a second ransomware attempt post-Greenlight.

<40 hours average time to full containment.