halcyon

Data Sheet

Halcyon + Backups: Better Together

Backups Are Necessary. But It's Not a Ransomware Resilience Strategy.

Backup tools were designed to help organizations recover from accidental deletion, hardware failure, and natural disasters. Ransomware is none of those things. It is a coordinated, multi-stage operation built to exfiltrate data, destroy recovery options, and inflict maximum business disruption before demanding payment.

The result is a ransomware resilience gap leaving businesses exposed even with backup infrastructure in place. When attackers get through, backup tools face a number of problems they were never designed to solve.

How Ransomware Defeats Backups

01. STEAL DATA BEFORE ANYONE NOTICES

During the dwell period, attackers quietly exfiltrate valuable data over days/weeks before triggering alerts. Restoring from backup recovers encrypted files, but it does not recover any stolen data. The impacts of breach notifications, customer exposure, and double extortion remain on the table no matter how clean the recovery.

02. FIND AND DESTROY THE RECOVERY OPTION

Immediately before triggering encryption, attackers neutralize backup infrastructure via retention policy manipulation, catalog deletion, time synch exploits, and direct service termination. Sophos found that 94% of ransomware attacks attempted to compromise backups with 57% succeeding.

03. COUNT ON THE BACKUP RESTORING THE SAME WAY IN

Backup captures the state of the environment at a point in time, including its weaknesses. Restoring without first identifying and closing the initial access path hands the attackers a ready-made second opportunity before operations are back online. A recent study found that 78% of organizations hit with a ransomware attack were hit again later.

04. USE RECOVERY DOWNTIME AS A WEAPON

With backup neutralized and encryption complete, attackers count on weeks of painful downtime to force a ransom decision. According to Gartner, the average organization spends 22 days recovering while Total Assure saw that number increase to 38 days in enterprise environments.

Why Add Halcyon to Your Backup?

Backup platforms are supposed to recover data. Halcyon ensures that recovery actually works, providing:

- **Backup Tamper Protection:** Halcyon monitors attempts to disable or corrupt your backup infrastructure before attackers can destroy it.
- **File Resilience:** Halcyon identifies active encryption processes and reverses them as they occur, preventing encryption from completing.
- **Encrypted File Recovery:** Halcyon captures encryption key material to decrypt impacted files and systems without relying on backups, reducing recovery time from weeks to minutes.
- **Data Exfil Protection (DXP):** Prevents data theft used in double extortion attacks, so backup recovery is not undermined by stolen data.
- **24/7 Ransomware Operations Center (ROC):** The Halcyon ROC manages detection, response, and recovery on your behalf at no additional cost, compressing recovery from days or weeks to minutes.

Halcyon vs. Backup Alone: What Changes

CAPABILITY	BACKUP ALONE	HALCYON + BACKUP
Backup Protection	Attackers neutralize backups through retention policy manipulation, catalog deletion, NTP exploits, and direct service termination.	Halcyon detects ransomware before it reaches backup infrastructure and monitors for attempts to disable or corrupt backup systems.
Encryption Prevention and Containment	Encryption spreads unchecked until alerts fire, maximizing data loss and the scope of recovery.	Halcyon identifies active encryption processes and reverses them in real time, preventing encryption while inoculating the environment limiting spread.
File Recovery w/o a Full Restore	Encrypted files require a full restore cycle taking days to weeks, assuming backups survived.	Halcyon captures encryption key material mid-attack, enabling the ROC to decrypt affected files in minutes.
Recovery Scope	With backup as the only recovery path, organizations face a full enterprise rebuild from a clean room: weeks of work with incomplete data recovery.	By preventing mass encryption and containing the blast radius, Halcyon shifts recovery from an enterprise-wide rebuild to targeted restoration of a few affected systems, compressing recovery time and data loss.
Exfiltration Coverage	Backup recovers encrypted files only. Data stolen before encryption is unaffected by any restore.	Halcyon DXP stops data theft before it leaves the environment, so backup recovery is not undermined by stolen data.
Managed Response	Incident response requires a separate engagement at significant additional cost, often with delayed availability.	The 24/7 Halcyon Ransomware Operations Center (ROC) investigates, responds, and leads recovery on your behalf at no additional cost.

Backup Is Not Enough. Halcyon Makes It Work.

Halcyon fills that gap that ransomware operators exploit. By detecting ransomware before it reaches backup infrastructure, reversing encryption as it occurs, capturing key material to recover affected files in minutes, containing the blast radius to limit what needs to be restored, reducing recovery time from weeks to hours or minutes, and providing 24/7 expert-led response at no additional cost, Halcyon transforms backup from a last resort into a reliable part of a ransomware-resilient posture.

The result is less data lost, fewer systems requiring full restoration, and recovery measured in minutes and hours rather than weeks.

The Bottom Line

Backup tools were built for accidents. Ransomware is not an accident, it's a coordinated attack designed to steal data, destroy recovery options, and hold your business hostage. Backup alone can't stop it.

Halcyon fills the gap. By protecting backup infrastructure from tampering, reversing encryption as it happens, capturing key material to recover files in minutes, blocking data exfiltration, and providing 24/7 expert-led response at no additional cost, Halcyon transforms backup from a last resort into a foundation for true ransomware resilience.

Backup is necessary. Halcyon makes it work.

Learn more at www.halcyon.ai