halcyon

Data Sheet

Ransomware Resilience for macOS

Running macOS Systems? Don't Leave Them Exposed.

Windows is still the top ransomware target, but Mac is growing fast. As organizations expand Mac deployments across their environments, attackers follow. A single unprotected Mac sitting in an otherwise well-defended, mostly-Windows fleet is still a foothold, and once an attacker has one, the operating system underneath it no longer matters. What matters is what they can reach from it.

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.

Key Features and Benefits

- Your business keeps running, even when ransomware hits.
- Ransomware-native defense designed to catch what generalist security tools miss.
- Recover in minutes, not weeks if an attack is successful.
- File Resilience makes it virtually impossible for attackers to encrypt your data.
- Prevent data exfiltration and double extortion.
- Get 24/7 monitoring from the world's first ransomware-dedicated SOC.

Supported Operating Systems

The Halcyon agent supports the following macOS versions on Apple Silicon.

- macOS 14 Sonoma
- macOS 15 Sequoia
- macOS 26 Tahoe

Comparing Windows and macOS Ransomware Attacks

Every ransomware attack has the same goal: apply enough pressure to force the victim to pay. Windows and macOS attacks just get there differently.

ATTACK STAGE	IMPACT ON WINDOWS OS	IMPACT ON MAC OS
Initial Foothold	Typically gained via phishing emails, malicious attachments, or drive-by downloads exploiting Windows vulnerabilities (e.g. SMB).	Often gained via Trojanized installers, malicious disk images (DMGs), phishing links, or misconfigured remote access services.
Privilege Escalation	Exploits Windows-specific vulnerabilities (e.g., EternalBlue) or abuses built-in tools like PowerShell and WMI.	May abuse TCC (Transparency, Consent, and Control) bypass techniques or exploit vulnerable third-party software running with elevated permissions.
Lateral Movement	Leverages Active Directory to spread across the network; uses tools like RDP, SMB, or PsExec.	May exploit shared credentials, SSH access, or cloud-sync services to spread across connected devices.
File Encryption	Targets common file formats (e.g., .docx, .xlsx, .jpg) and encrypts them with ransomware-specific keys.	Encrypts user and application data, commonly targeting home directories and cloud-sync folders (e.g., ~/Documents, ~/Desktop).

ATTACK STAGE	IMPACT ON WINDOWS OS	IMPACT ON MAC OS
Persistence Mechanisms	Installs backdoors or registry entries to ensure the ransomware restarts even after a reboot.	May install LaunchAgents, LaunchDaemons, or login items to survive reboot.
Ransom Note Delivery	Displays a ransom note on desktop or as a startup message using Windows GUI tools or system logs.	Places ransom notes in key directories or alters login and desktop messages.
Ransom Demand	Ransom note demands payment in cryptocurrency, usually via a GUI popup or browser-based instructions.	Provides payment instructions in text files, typically without the GUI polish seen in Windows attacks.
Recovery Challenges	Recovery may require reinstalling the OS, restoring from backups, or using specialized decryptors (if available).	Recovery often relies on Time Machine backups or full OS reinstall, complicated by FileVault encryption interactions.

Got a Mac gap in your ransomware defenses? Close it, with Halcyon.

The Halcyon Anti-Ransomware Platform extends the same proactive, real-time ransomware protection your Windows and Linux environments already rely on to macOS endpoints. Whether you're protecting a handful of Macs in an otherwise Windows fleet or running a primarily Mac environment across the organization, Halcyon provides comprehensive defense against ransomware with minimal operational impact.

Macs have a reputation for being safer. That reputation formed when Macs sat outside the systems attackers cared about. Not anymore. Macs hold the same financial records, source code, and customer data, and whether Macs make up a fraction of your environment or all of it, unprotected endpoints are exactly what attackers are counting on.

Once an attacker has a foothold on a Mac, the attack still has to progress the same way it would anywhere else. In most ransomware attacks today, the goal isn't to choose between stealing data and encrypting it, it's to do both. Exfiltrating data first and then encrypting it applies maximum pressure: even if a victim can restore from backup, the threat of leaked data still forces the ransom conversation. Halcyon is positioned at both stages of that pressure campaign. Halcyon Data Exfiltration Protection detects suspicious data movement, catching theft before it completes. If the attacker also attempts encryption, Halcyon detects that process as it's happening and stops the changes before they're ever written to disk. Halcyon makes your files virtually unencryptable. The attack doesn't get cleaned up after the fact. The attack never finishes.

Every attempt also makes the rest of your environment harder to hit. **The moment Halcyon identifies the tactic behind an attack on one endpoint, that intelligence is pushed out to every other device under protection, Mac, Windows, or Linux, so the same technique is already recognized and stopped before it reaches a second machine.** And behind all of it is Halcyon's Ransomware Operations Center (ROC), a dedicated team of ransomware experts monitoring every endpoint 24/7/365 at no additional cost, so nothing here depends on business hours or on someone noticing in the moment.

Ransomware will come for your business. Halcyon makes sure it doesn't win on Windows, Linux, and Mac. **See Halcyon for macOS in action. Visit halcyon.ai and schedule your demo today.**