halcyon

Data Sheet

Your Servers Are the Crown Jewels. That is Exactly Why Ransomware Never Starts There.

Ransomware operators do not break through server-side defenses. They walk past them, using harvested credentials from the endpoints that your servers-only posture was never watching. By the time encryption begins, the campaign is already over.

How Modern Ransomware Actually Works

Today's ransomware is an intelligence-driven operation, not a malware event. Operators spend weeks on your endpoints before they ever touch a server, harvesting credentials, mapping backup infrastructure, and quietly exfiltrating data.

Ransomware Starts with Your Everyday System Access

High-value credential holders on endpoints

- Help desk staff with admin credentials
- Finance teams authenticated into Oracle or SAP
- Procurement teams with access to Workday and banking platforms
- IT admins with domain-level privileges

Attack surfaces your servers-only posture cannot see

- VDI sessions linking endpoints directly to data repositories
- Managed workstations with trusted paths to file servers
- Backup infrastructure mapped and destroyed from the endpoint
- Exfiltration staged silently before the ransom note is written

The Real Attack Path

Endpoint Entry

Workstation, laptop, or remote device is compromised via phishing, exposed RDP, or supply chain.

Credential Harvest

Admin, finance, and IT credentials stolen from help desk, ERP, cloud, and banking platforms.

Lateral Movement

Attacker becomes a trusted insider, disabling security tools and destroying backup paths.

Server Detonation

First moment server-only coverage sees anything. Every recovery path is already gone.

Steps 1-3 run entirely unmonitored, in a server-only posture.
By step 4, ransomware resilience is no longer an option, only damage control.

The Numbers Behind the Risk

40%

of victims had attackers lurking undetected for 8-30 days before detonation. (Omdia Technical Validation, 2026)

22 Days

average industry-wide restoration timeline using backups, assuming backups survived at all (Industry average)

95%

despite having full confidence in detections, still failed to stop a ransomware campaign (Omdia, 400 orgs, 2026)

49%

of victims detected their last attack too late to prevent significant damage (Halcyon Security Leadership Survey)

The Question Worth Sitting With

"Are you relying on old assumptions made before backup destruction became an attack methodlogy?"

What Each Phase Looks Like in a Server-only Deployment

Dwell Time Phase	Operations Halt Phase	Recovery Phase
Weeks Before	**Hour 0**	**Days 1 to 22+**
• Endpoint compromise goes completely unmonitored • Credentials harvested to disable security tooling • Backup infrastructure mapped for destruction • Data staged and exfiltrated before any ransom note	• First moment servers-only coverage detects anything • Decision authority passes entirely to the attacker • Ransom demand lands with deadline already running • Every recovery path already compromised	• Encryption keys only capturable at point of encryption • Encryption begins on endpoints, not servers • Missed endpoint = missed recovery window • Ransom negotiation runs in parallel with restoration

The Recovery Gap That Closes at the Endpoint

Scenario	Servers-Only Posture	Halcyon Full Fleet
Detection confidence	95% of confident organizations still failed to stop the attack.	Purpose-built to cover the gaps EDR was never designed to close.
Encryption key capture	Not possible. Encryption begins on endpoints outside coverage.	Keys captured at the point of encryption.
Recovery timeline	22-day industry average, if backups survived destruction.	Recovery in minutes with automated key-based decryption.
Dwell time	Completely blind to credential harvest and lateral movement.	Behavioral coverage across the full chain from first access onward.
Backup destruction	Backup mapping and destruction runs undetected across endpoints.	Exfiltration prevention and ransomware behaviors flagged early.

Why Halcyon Closes the Gap: Built Exclusively for Ransomware. Not Adapted for It.

Key Material Capture: Encryption keys are captured at the moment encryption begins on the endpoint, enabling decryption without paying the ransom regardless of backup status.

Omdia Validated: "EDR solutions have not been designed to tune into the specific behaviors of ransomware attacks." Omdia Technical Validation, February 2026.

Ransomware-Specific Detection: Purpose-built to catch behaviors that look like legitimate administration, because ransomware operators specifically train to avoid triggering generic EDR alerts.

Exfiltration prevention: Detects data staging and exfiltration before the ransom note is written, eliminating the double-extortion leverage operators use to maximize pressure.

Where Do We Go From Here

The threat has changed. Most deployment postures have not. If yours was built before data exfiltration became the opening move and backup destruction became standard methodology, that is the conversation worth having. Bring your stack and your recovery plan. We will show you exactly where you are covered and where you are not.

The Halcyon Anti-Ransomware Platform. Full fleet coverage — Zero recovery downtime. Schedule an executive briefing at halcyon.ai