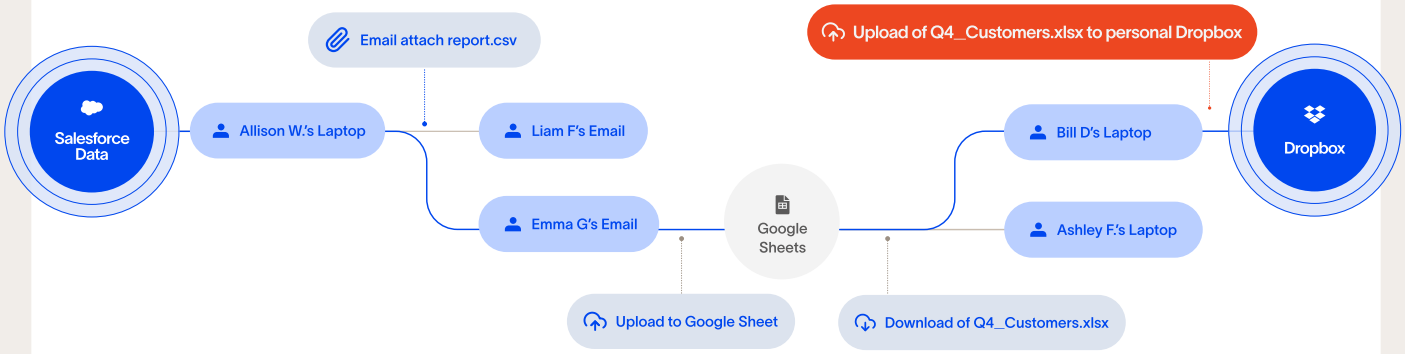
cyberhaven

How to Stop Data Exfiltration Everywhere It Happens

Legacy DLP misses the channels attackers and insiders actually use. Here is what AI-native, modern endpoint DLP covers from the platform built for Data Security for the Agentic Enterprise.

Data exfiltration does not follow rules. It happens when someone copies a file to a USB drive, pastes customer data into an AI application, or uploads a document to a personal cloud account. Legacy DLP uses static, content-based rules that fire on volume, not context, generating noise instead of signal. Now AI agents act on data at machine speed, turning any coverage gap into an entry point for data loss. Modern endpoint DLP stops exfiltration where it happens.

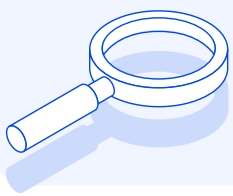


The 6 Exfiltration Channels DLP Must Cover

Channel	What legacy DLP misses
Endpoint (USB, print, AirDrop)	Blocked before data leaves device
Encrypted/compressed files	Data tracked through obfuscation
Certificate-pinned apps (Dropbox, WhatsApp)	Invisible to CASB and web proxies
Personal cloud accounts	Personal vs. corporate instance distinction
Email and web	Unified policy across all channels
AI (ChatGPT, Copilot, etc.)	Visibility into GenAI applications and endpoint-based agents, with every agent action tied to an identity

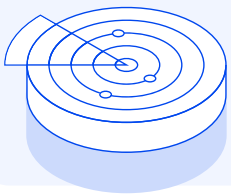
How Cyberhaven DLP Works

01 Discover



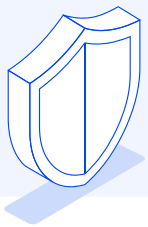
Trace the full lifecycle of your data from its origin, classifying it by content and context without waiting for policies or manual tags.

02 Monitor



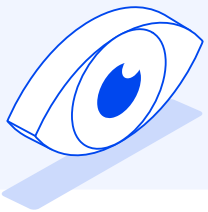
See how humans and AI agents create, copy, fragment, and share data across endpoints, browsers, and cloud apps in real time.

03 Protect



Block, warn, or coach at the moment of action, adapting protection as context changes to stop risk before it becomes loss.

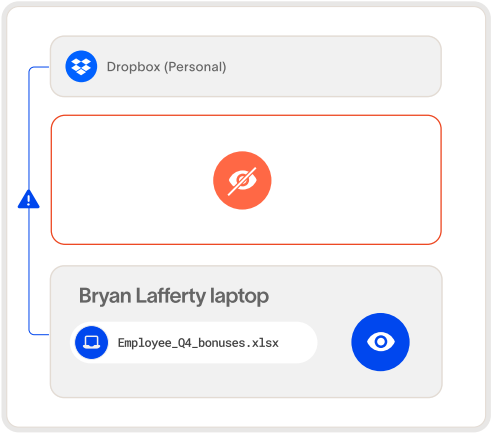
04 Investigate

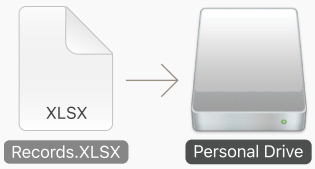


Follow the complete, defensible record behind every incident, with data lineage showing who touched what, when, and where it went.

Key Capabilities of DLP

- Block endpoint exfiltration (USB, printers, AirDrop, Bluetooth)
- Close network blind spots (certificate-pinned and E2E-encrypted apps)
- Coach users in real time with instant warnings
- Collect forensic proof (file history, clipboard, screenshots)
- Track data lineage through encryption and compression





Why the Endpoint?

Exfiltration does not happen in the cloud at rest. It happens at the endpoint, where humans and AI agents act on data and where every channel is visible in one place.

Data Security for the Agentic Enterprise

Request a demo

cyberhaven.com/request-demo

Cyberhaven is a leader in Data Security for the Agentic Enterprise, trusted by the world's most innovative companies to protect their most sensitive data. AI changed work. Cyberhaven protects it. Learn more at cyberhaven.com.