cyberhaven

DATASHEET

Stop Sensitive Data Loss *Without* Slowing Down the Business

Security teams at the world's most innovative companies use Cyberhaven to understand the full journey of every sensitive file, from creation through every app, device, and destination, so they can prevent data loss with confidence, precision, and dramatically fewer false positives.

THE CHALLENGE

Why Traditional DLP Falls Short

Traditional DLP and insider threat solutions consistently disappoint, drowning security teams in false alarms while critical data breaches slip through undetected. These outdated tools rely entirely on content inspection, missing important data that contains no recognizable content pattern. Meanwhile, they disrupt legitimate work activities and frustrate employees with excessive restrictions.

Legacy DLP was built for a different era. It inspects files at a single point but has no visibility into how data moves between apps, who accessed it first, or where it originated. In a world where sensitive files touch dozens of cloud and AI applications before reaching a risky destination, this approach leaves enormous blind spots. And when incidents do surface, analysts spend more time assembling context from scattered consoles than actually investigating threats.

THE CYBERHAVEN APPROACH

Data Lineage Meets *AI-Powered* Protection

Cyberhaven traces the complete journey of every sensitive file from its original source through every app, user, and destination. By combining AI-powered content inspection with data lineage, Cyberhaven builds a real-time graph of data movement that distinguishes legitimate business activity from genuine risk. The result: precise protection that traditional DLP simply cannot deliver.

KEY OUTCOMES

Slash False Positives by 90%

Stop wasting analyst time on noise. By combining content analysis with data lineage, where data originated, where it's been, and who handled it, Cyberhaven dramatically reduces false positives.

Catch Data Theft Before It's Too Late

Detect exfiltration the moment it begins. Real-time policies block sensitive data across all channels, email, cloud, USB, GenAI, while educating users on acceptable behavior.

Investigate in Seconds, Not Hours

Accelerate analyst workflows with full incident timelines and pre-built security workflows. AI-powered agents turn multi-step investigations into natural-language queries.

Protect Data Beyond Content Inspection

Source code, product designs, recorded meetings, business plans, data lineage identifies and protects what content inspection alone misses, including encrypted and compressed data.

Simple Policies, Better Results

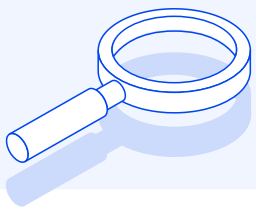
Define policies with an intuitive visual editor. Test against historical data to preview results instantly. One lineage-powered policy replaces dozens of brittle content rules.

Secure AI Usage Across the Org

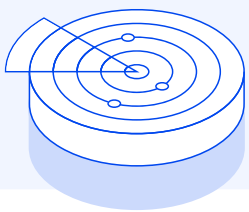
Achieve unprecedented visibility into shadow AI usage. Monitor data flowing to GenAI tools and prevent sensitive information from reaching unapproved AI applications.

HOW IT WORKS

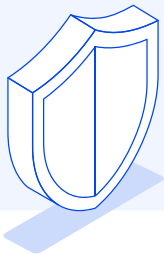
01 Discover



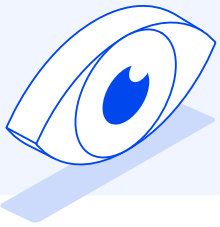
02 Monitor



03 Protect



04 Investigate



CORE USE CASES

Data Exfiltration
Prevent sensitive data from leaving by enforcing controls across all major exfiltration channels.

Departing Employees
Flag high-risk users and review historical activity to the point and time of data exfiltration.

Insider Threats
Identify high-risk behaviors and take instant, automated actions to stop data loss.

M&A Data Risks
Monitor and enforce controls to stop the unauthorized sharing of confidential information.

Accelerate SecOps
Leverage AI and pre-built analyst workflows to detect risks missed by traditional policies and speed up incident response.

Shadow AI
Achieve unprecedented visibility into AI usage and enforce risk-based controls across GenAI tools.

PLATFORM CAPABILITIES

Real-Time Data Lineage
Discovers hundreds of AI tools across endpoints, browsers, CLIs, and IDEs; existing and emerging, standalone and embedded, personal and corporate accounts.

Data Lineage for AI
Traces data origin, movement, and transformation across every AI interaction. Connects agent actions to data for full forensic context.

AI Usage Insights
Adoption trends, power users, sensitive data shared with AI, and protections applied from a single console.

Agentic AI Discovery
Reconstructs full execution lifecycles for Claude Code, Codex, Copilot, and other agents, including tool calls, data access, API invocations, and multi-turn context.

AI Data Flow Control
Runtime guardrails block, warn, or redact at the prompt and response level. Plain-English risk explanations replace generic block pages.

AI Risk IQ
Scores AI apps and agents across five dimensions: data sensitivity, model integrity, compliance adherence, user access, security infrastructure.

INTEGRATIONS & PLATFORM COVERAGE

Cloud Storage: Google Drive, OneDrive, Dropbox, Box, SharePoint **Communication:** Slack, Teams, Gmail, Outlook, Zoom, Webex **Dev Tools:** GitHub, GitLab, Jira, Confluence **GenAI:** ChatGPT, Copilot, Gemini, Claude, Perplexity **SIEM/SOAR:** Splunk, CrowdStrike, Palo Alto, Okta **Cloud:** AWS, Azure, GCP **Endpoint:** Windows, macOS **AI Analyst:** Claude Code, Codex, any MCP-compatible client

RESULTS CUSTOMERS LOVE

90%
Reduction in false positives

5x
Faster incident investigation

80%
Fewer incidents with user coaching

Request a demo

About Cyberhaven

Cyberhaven pioneered data lineage for enterprise security. Trusted by leading enterprises across financial services, technology, healthcare, and government, Cyberhaven delivers unified data security, DLP, DSPM, IRM, and AI Security, from a single platform.