cyberhaven

Proactive Insider Risk Management

Until now, insider risk products have taken a passive approach — they alert you to threats but don't stop them, and too many of their alerts are false positives. Cyberhaven combines data awareness and behavioral signals to detect and stop insider threats and protect important data, across human and agentic workflows.

The Limits of Traditional IRM

Only analyzes behavior, not the data being handled

IRM tools look at behavior but can't connect it to what data is being handled or events across time. They generate alerts for things that aren't risky while missing many actual insider threats.

Cannot intervene and stop data from leaving

When IRM tools detect a user mishandling data, they only send an alert. They're designed to ingest event logs and analyze them but they don't have a footprint to take action when data is at risk.

Sends alerts that lack context to investigate

In order to understand the user's intent, security analysts investigating a potential incident often need to hunt for additional details beyond what an alert from an IRM tool provides them.

Cyberhaven Redefines IRM

We don't just accurately detect insider threats. Cyberhaven intervenes the moment data is at risk to protect it, then we give security analysts everything they need to quickly investigate.

Combine behavioral analysis with data analysis to accurately detect threats

Knowing what data is involved makes detection more sensitive to real threats and quieter on everyday behavior.

Identify threats that unfold over weeks or months, not just hours

Events are retained and correlated across weeks or months, the way real insider threats unfold.

Don't just accurately detect insider threats, stop them

Blocks exfiltration across every channel, including cloud, email, websites, removable storage, and Apple AirDrop.

Educate users on appropriate behavior in the moment using real-time popups

Real-time coaching at the moment of a risky action is more effective than after-the-fact notifications.

Collect forensic-level events without physical access to a device

Every user action is captured remotely and stored securely in the cloud for post-incident investigation.

Give analysts the context needed to quickly understand user intent

An incident response view traces every step leading up to an event, separating carelessness from malicious intent.

Our Unique Advantages: The Magic Behind Cyberhaven

Data Lineage

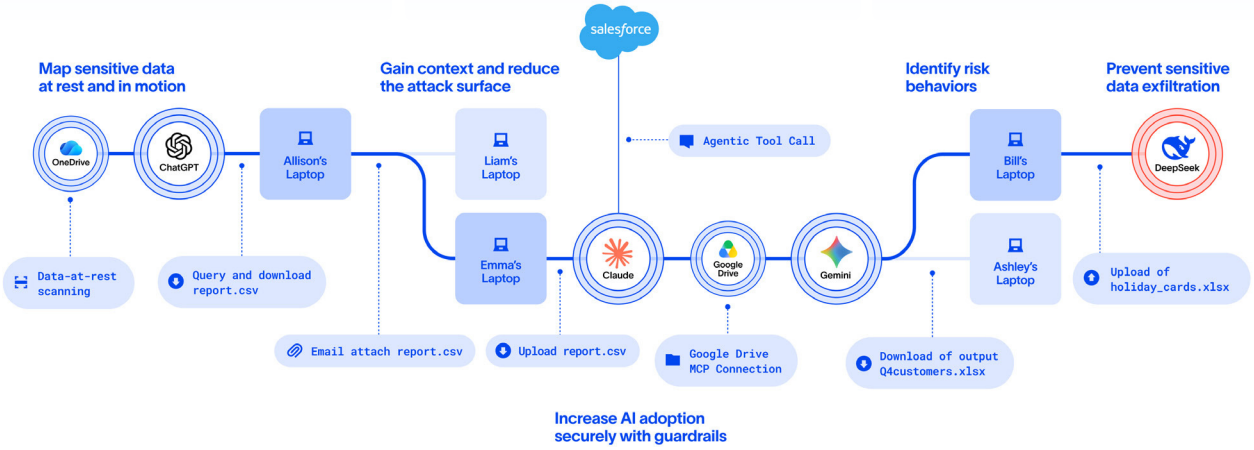
Traces the complete flow of data, providing vital context about where the data came from, who's interacted with it, and how it's been modified over time.

AI Classification

Applies advanced AI to lineage, context, and content, achieving dramatically higher accuracy and more effective enforcement.

Agentic AI

Cyberhaven Linea AI agents precisely analyze billions of workflows and every piece of data to find and report on insider risks.



Everything Else You Expect From IRM

When we set out to redefine IRM, we included the standard features you expect.

- Collect user behavior across platforms
- Flag filename or extension changes
- Track changes to sharing permissions
- Forensic file capture
- SIEM integration and APIs
- User directory integration
- Screenshot capture
- Role-based access control
- Distinguish personal and corporate app instances
- User watchlists and elevated remediation
- Reporting and analytics

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.