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.

The limits of traditional insider risk management

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

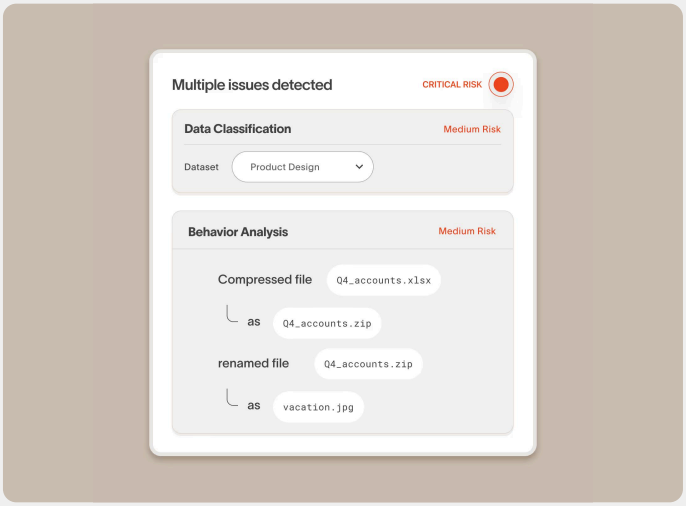
In order to understand the user's intent, security analysts investigating a potential incident often need to hunt for additional details beyond what an alert from an IRM tool provides them.

Cyberhaven redefines insider risk management

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.

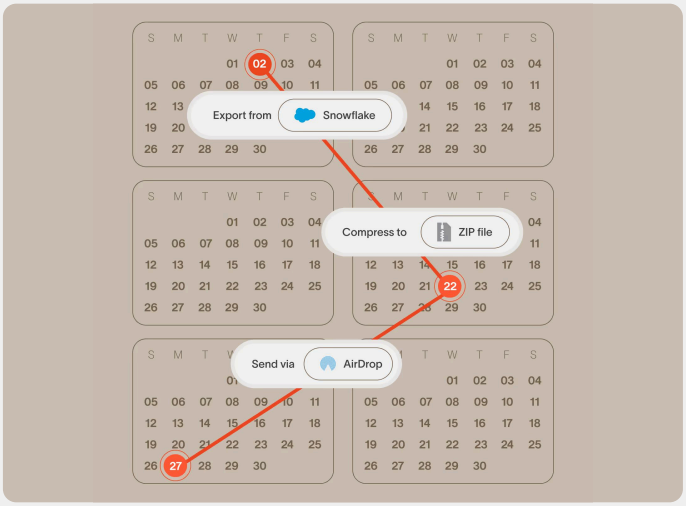
Combine behavioral analysis with data analysis to accurately detect threats

Cyberhaven precisely distinguishes between an employee performing an action with important corporate data versus personal/unimportant data. This additional dimension makes us more sensitive to actual insider threats while allowing us to ignore many everyday behaviors that aren't risky.



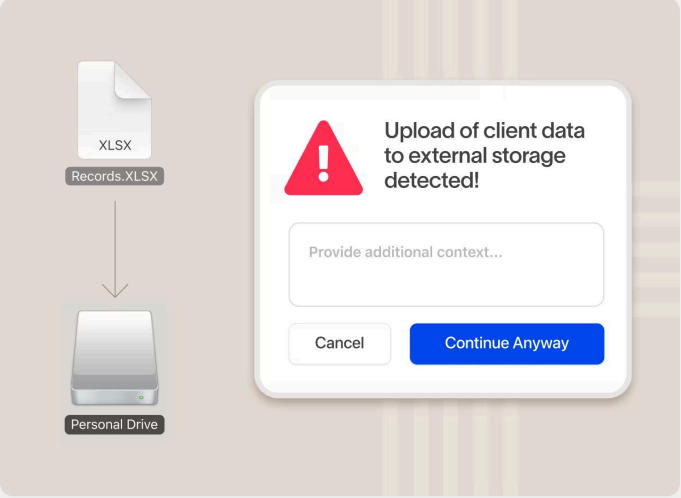
Identify threats that unfold over weeks or months, not just hours

Cyberhaven stores a record of events indefinitely and we can correlate events occurring weeks or months apart, which is how many threats happen in the real world.



Don't just accurately detect insider threats, stop them

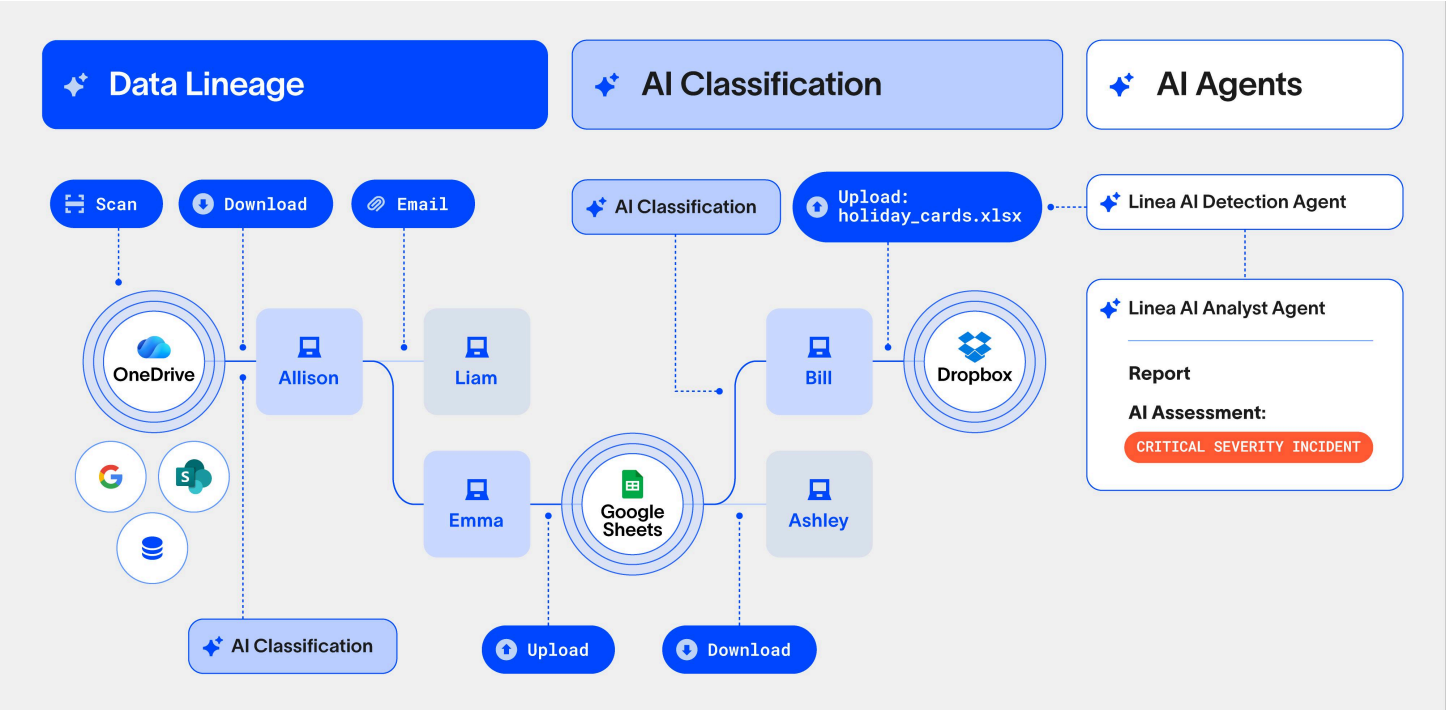
Cyberhaven is built to take immediate action when there's an insider threat in progress to prevent someone from taking important data. We block data exfiltration across all channels including cloud, email, websites, removable storage devices, Apple AirDrop, and more.



cyberhaven

The Magic behind Cyberhaven is Data Lineage

Data lineage is a technology that's only available from Cyberhaven that powers best-in-class identification and protection of sensitive data.



Where it originated

Whether the customer database in Snowflake or the product design in Figma, different types of data originate in different places.

How it was handled

Data moves in recognizable ways, passing through the board meeting site in SharePoint or the employee offer letter account in DocuSign.

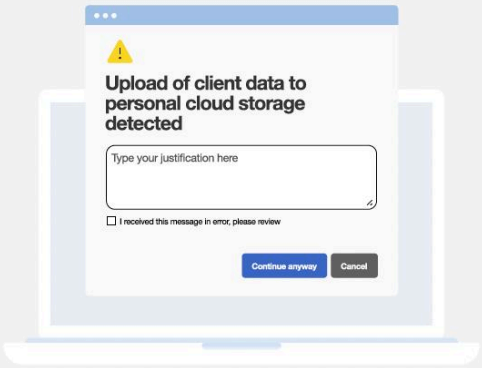
Who interacted with it

Different employees produce different work, from researchers who develop drug formulas to designers working on new products.

cyberhaven

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

The best security starts with an educated workforce. When an employee does something risky we can show a popup message coaching them in the moment, which is more effective than email notifications.

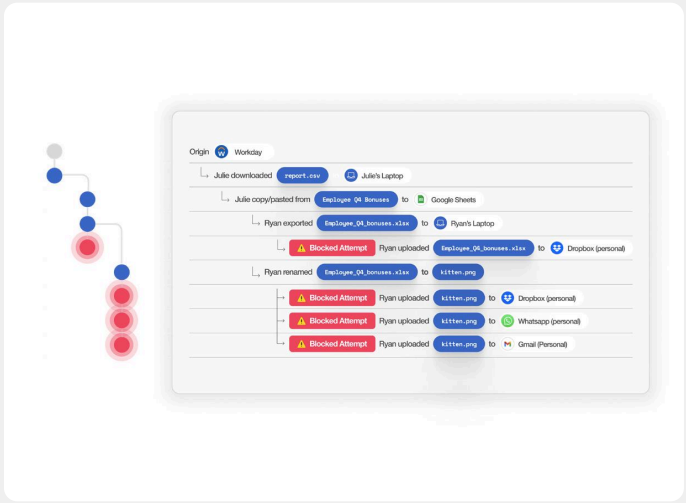


Collect forensic-level events without physical access to a device

We remotely capture every user action related to every piece of data and securely store it in our cloud so you can perform a post-incident investigation without needing physical possession of a device.

Give analysts the context needed to quickly understand user intent

Cyberhaven provides an incident response view tracing every step and action related to a piece of data leading up to an incident, helping analysis quickly understand whether the behavior is due to carelessness or part of a pattern of malicious behavior.



Everything else you expect from an IRM solution

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

Collect user behavior across platforms

Collects user behavior across cloud, devices, messaging, email, apps, and more and correlates related events across platforms.

Flag filename or extension changes

Flags when a user changes the extension or name of a file that contains sensitive data and can block subsequent exfiltration.

Track changes to sharing permissions

Tracks sharing permissions to individual users and also links that can be accessed by anyone in the organization or anyone with the link.

Forensic file capture

Incidents for content-based policies include a highlighted excerpt showing what triggered the policy. These matches are stored in the customer's cloud.

SIEM integration and APIs

Natively integrates to SIEM tools such as Splunk and exposes incidents through an API so you can add them to any third-party security tool.

User directory integration

Integrates with on-premises and cloud-based directory services to pull user details such as department, manager, and departure date.

Screenshot capture

Optionally record the user's screen in the seconds leading up to an incident. Screenshots are stored in the customer's cloud.

Role-based access control

Includes standard out-of-the-box roles or create your own custom roles with any combination of permissions.

Distinguish personal and corporate app instances

Distinguish between the corporate instance of an approved cloud application and a personal instance of the same application.

User watchlists and elevated remediation

Add users to watchlists and apply elevated response actions such blocking upload to unapproved destinations without allowing the end user to override.

Reporting and analytics

Includes out-of-the box dashboards and a fully customizable reporting engine for advanced analytics.

Go beyond IRM with Cyberhaven

Contact us at sales@cyberhaven.com to learn more.

cyberhaven