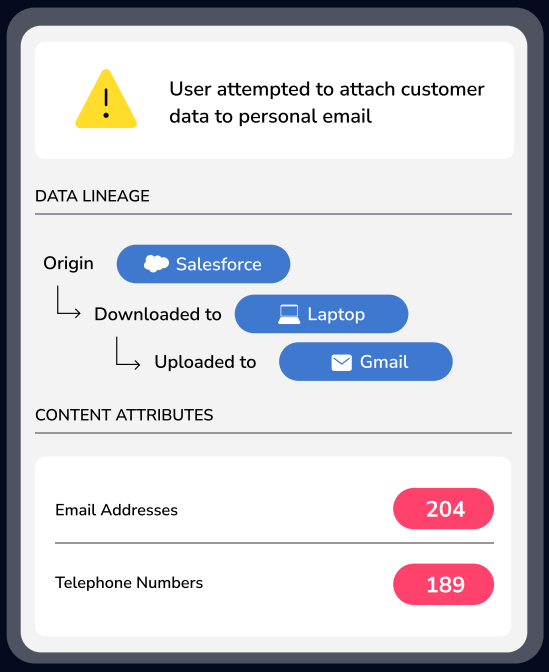
cyberhaven

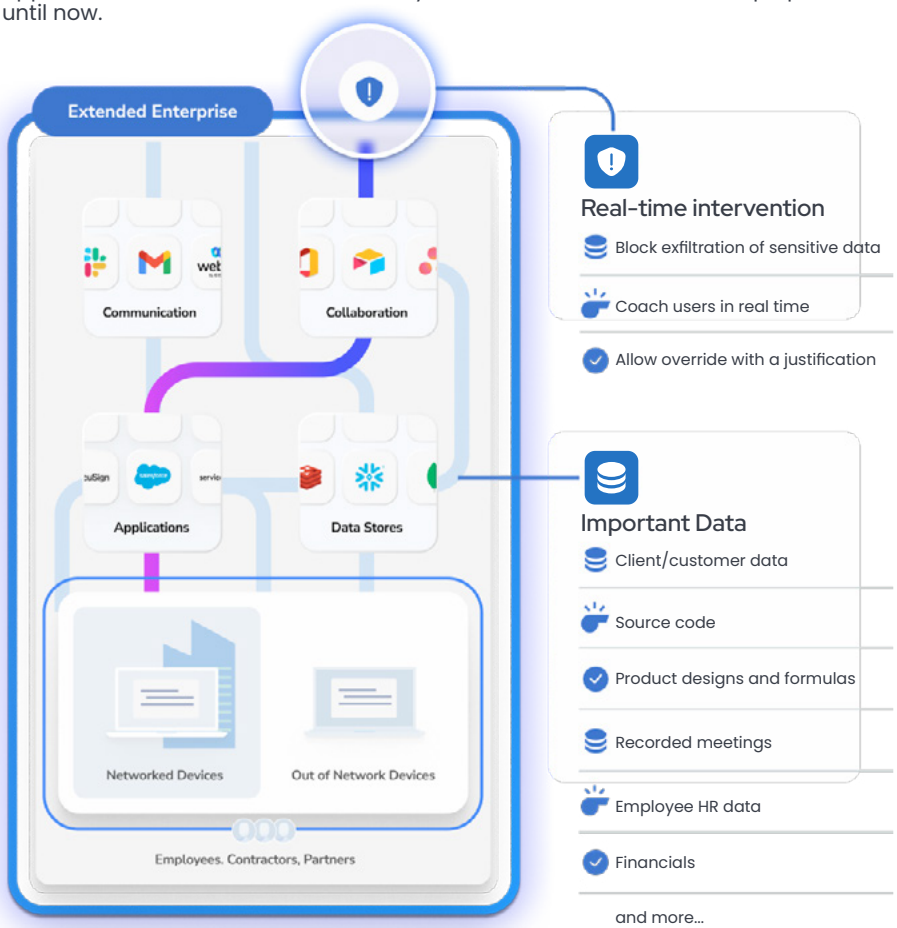
Cyberhaven Data Detection and Response

Cyberhaven Data Detection and Response (DDR) is a better way to protect your company's sensitive data from insider threats and accidental exposure.



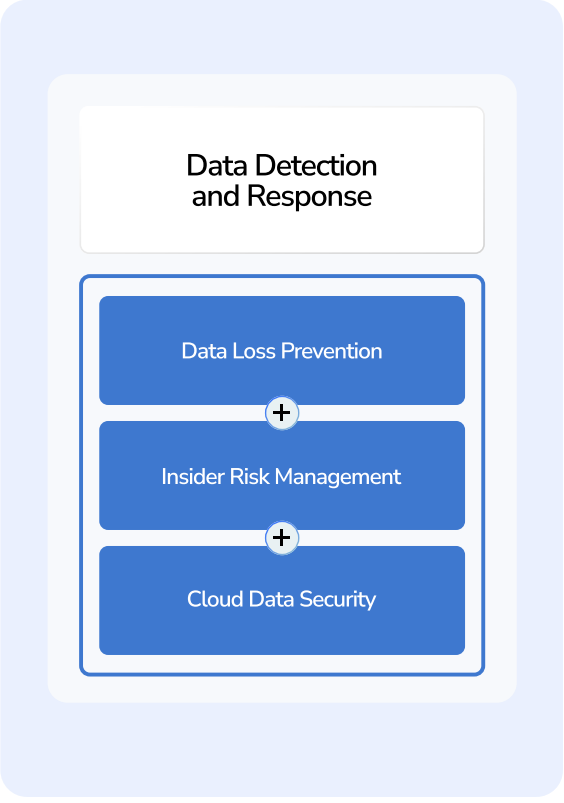
Protect data from insider threats and exposure across the extended enterprise

Your company's important data is always in motion, spreading to new people, applications, and devices. Data security tools have been unable to keep up — until now.



More than the sum of its parts: three data security products in one

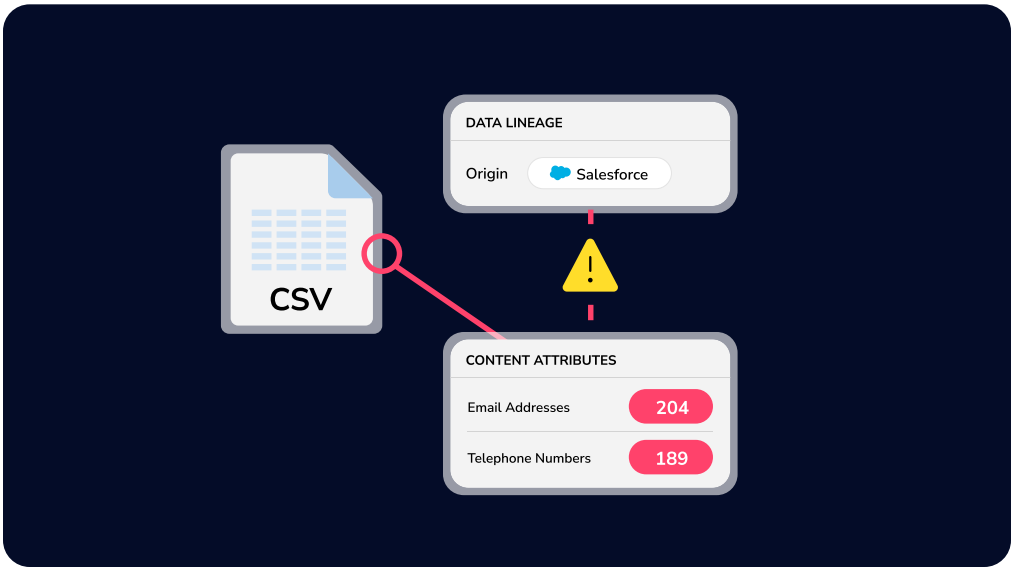
DDR combines and enhances the coverage of multiple tools, providing more effective data protection than using separate solutions.



cyberhaven

What Makes Us Different

Cyberhaven protects data other tools can't see, from threats they can't detect, across technologies they can't control.



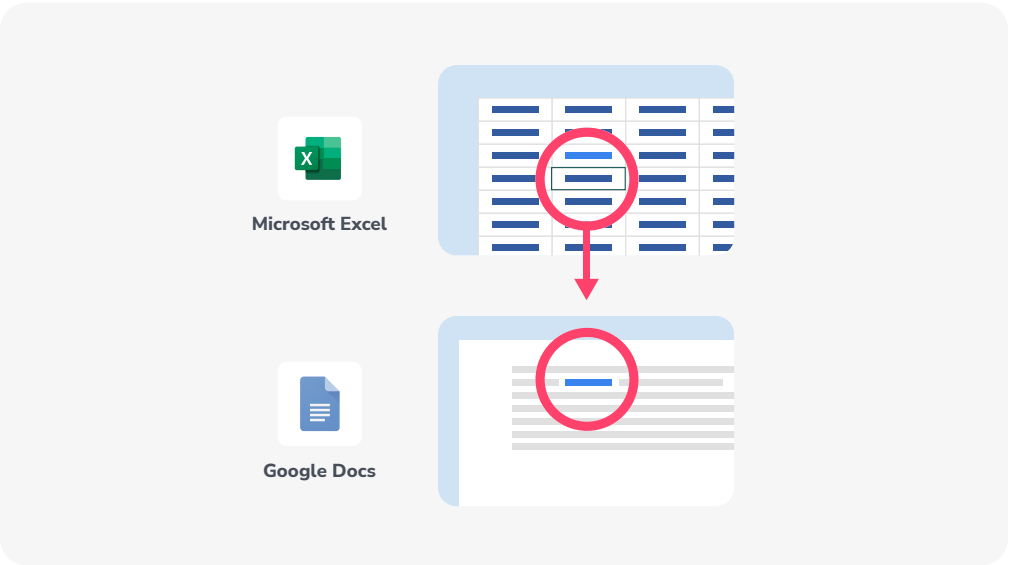
Combine content analysis and data lineage to classify data you can't using content alone

Reduce false positives

Many common content patterns DLP products look for are found in non-sensitive data, leading to false positive alerts. Cyberhaven combines content analysis and data lineage — where the data came from and where it's been — to more accurately classify data and reduce false positives by 95%.

Classify data you can't today

Many types of sensitive data don't contain recognizable words or patterns, or any text content at all. With data lineage, you can finally classify and protect any type of data.



Protect data at the most granular level with robust and thorough tracking out of file and sensitive data

Track data that doesn't live or stay in a file

Data classification tools tag files, and DLP tools track file origin, but neither can follow data copied out of a file or between apps. Cyberhaven tracks every fragment of data everywhere it goes.

Track sensitive data through obscuring efforts

Malicious insiders sometimes try to circumvent data protection solutions by compressing or encrypting a file. Cyberhaven always maintains the data's lineage — ensuring sensitive data remains protected.

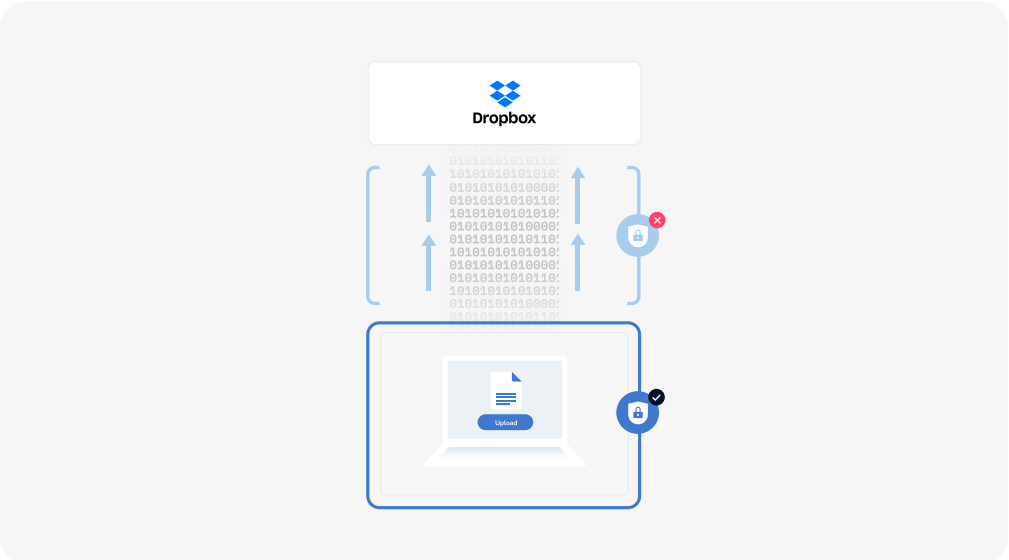
cyberhaven

What Makes Us Different Continued

Use both employee behavior and data intelligence to more accurately detect insider threats

Data-aware insider risk management

Insider risk management solutions are plagued by false positives because they are too focused on employee behavior. Cyberhaven can more accurately detect actual insider threats because we analyze behavioral signals combined with the true sensitivity of the data being handled.



Prevent data from going to unsanctioned apps by stopping it on the device, not the network

New forms of encryption require a new security approach

CASBs and web proxies can't decrypt traffic to cloud apps that use end-to-end encryption or certificate pinning — like Dropbox, Google Drive, and Whatsapp. Cyberhaven stops exfiltration to these apps before data is encrypted and sent.

cyberhaven

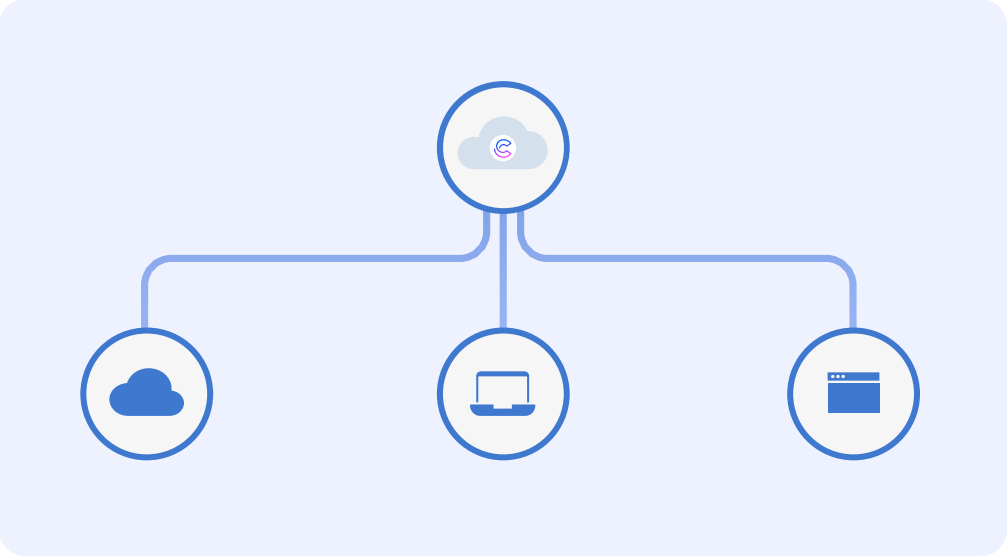
How It Works

Cyberhaven collects every event for every piece of data and connects these billions of events to classify and protect data anywhere it goes.

1

Collect all events for every piece of data

We don't just analyze the content of the data, we collect and analyze the events surrounding it.



Cloud API Connectors

Cyberhaven connects to sanctioned applications to get visibility into content created and shared natively in the cloud.

Modern, lightweight endpoint agent

Our endpoint agent utilizes operating system APIs to secure data without slowing computers.

Browser plugin

Cyberhaven supports all major browsers to provide visibility and control for web-based cloud applications.

CYBERHAVEN RECORDS EVERY EVENT FOR EVERY PIECE OF DATA

- Export report from app
- Copy/paste content
- Attach file to email
- Convert file to other format
- Upload file to cloud app
- Send via Airdrop
- Compress data in ZIP file

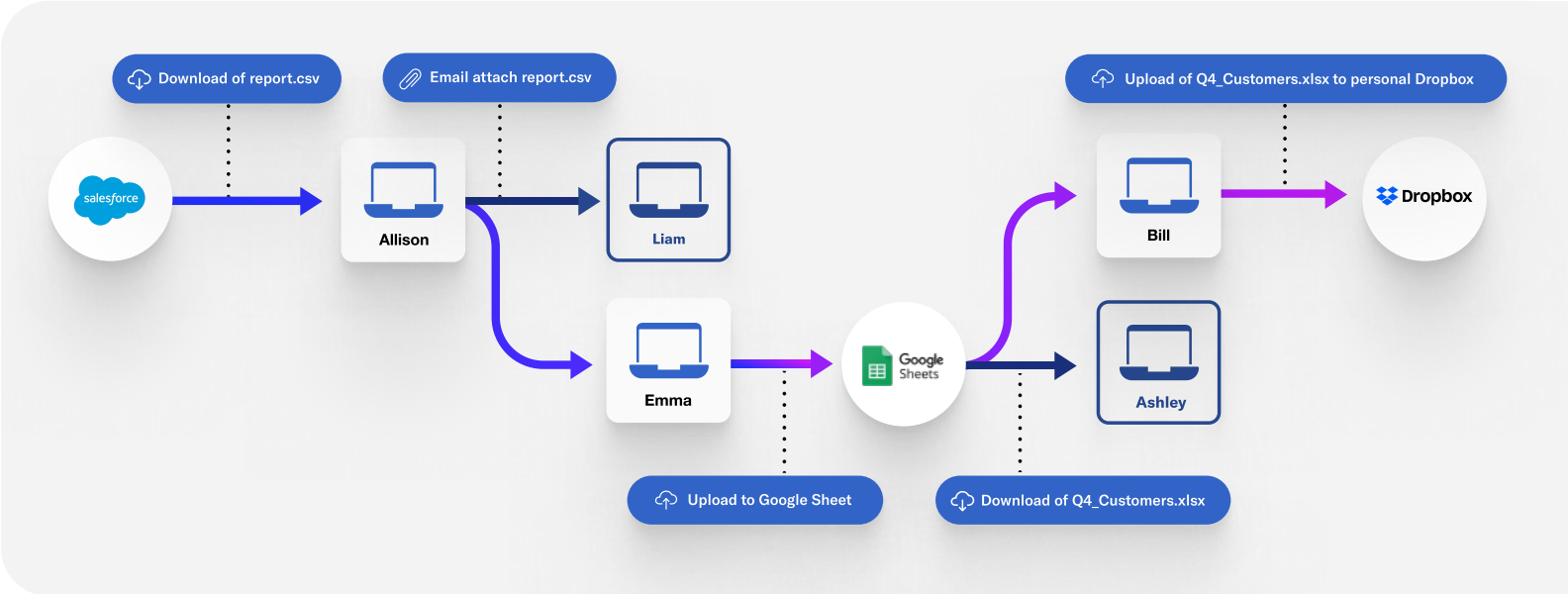
and more...

cyberhaven

2

Trace the data's lineage to classify and track it

We correlate all of these events in real-time and calculate the lineage for every piece of data from its origin and as it moves throughout your company.



THE POWER OF DATA LINEAGE

We use data lineage to discover important context allowing us to determine and track sensitivity

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.

Content Analysis and Third-Party Labels

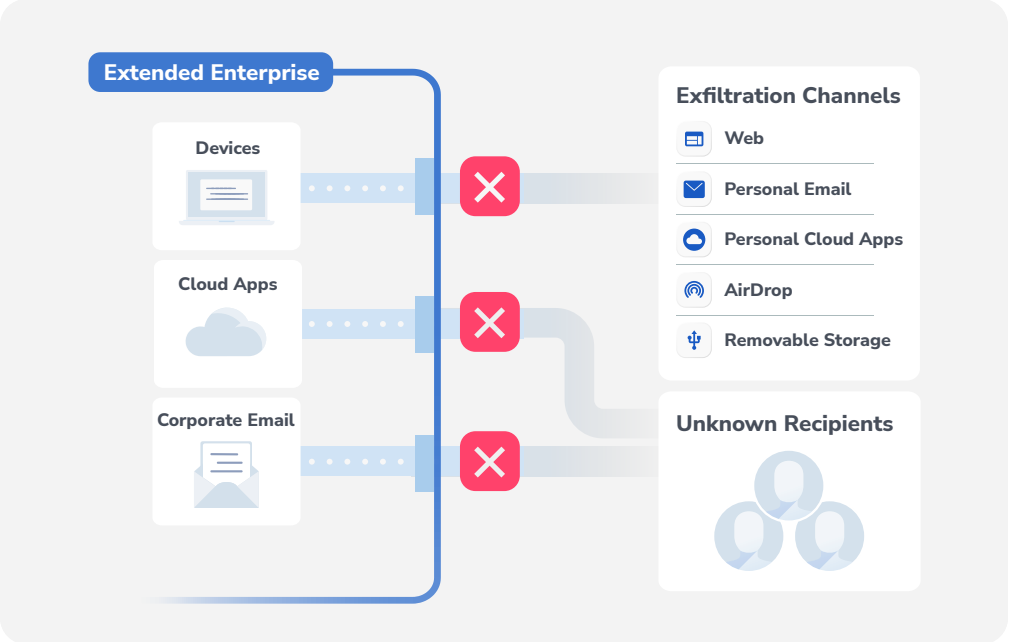
We combine the context gained from data lineage with content analysis. Cyberhaven includes out-of-the-box content identifiers for common forms of PII, PCI, and PHI along with the ability to define your own patterns using regular expressions. We can also read third-party classification tags/labels applied to files.

cyberhaven

3

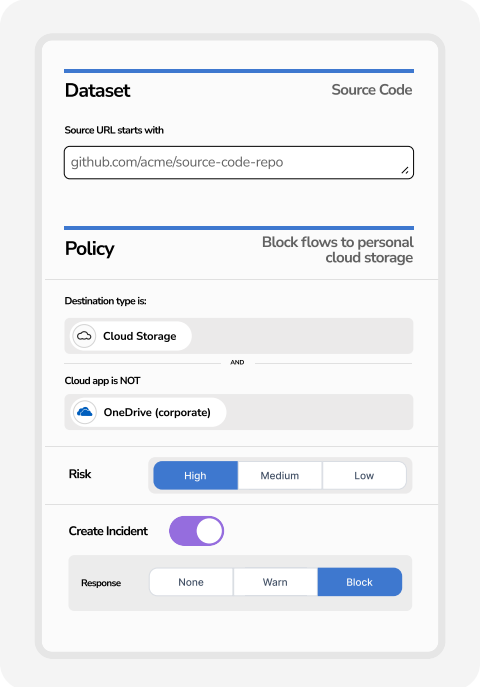
Enforce your data security policies

Cyberhaven policies allow you to define what is risky for your organization and enforce actions to protect data and educate your workforce in real time.



Stop data exfiltration across any channel

Cyberhaven's architecture enables data protection across all major exfiltration channels including web, cloud, email, AirDrop, USB devices, and printing.

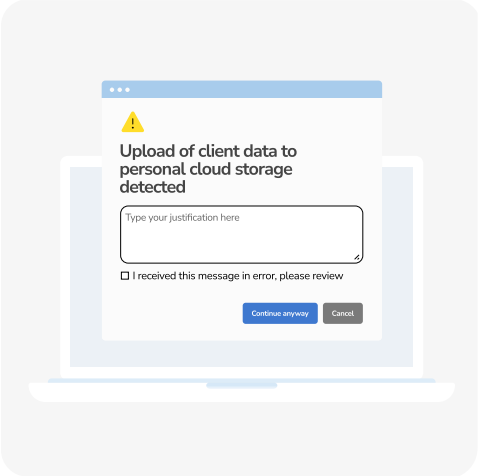


Tiered response based on severity

Cyberhaven can enforce tiered responses depending on the risk level of an action, the data involved, and the company's security culture.

Preview results before deploying policies

Because Cyberhaven stores all events for all data, you can preview violations that a new policy would have created across historical events — giving you confidence before you deploy.



Allow override with a business justification

Cyberhaven can enforce a policy like blocking data going to an unapproved destination, while still giving employees the ability to override in the case there's an approved business reason, so security doesn't get in the way of productivity.

Real-time education

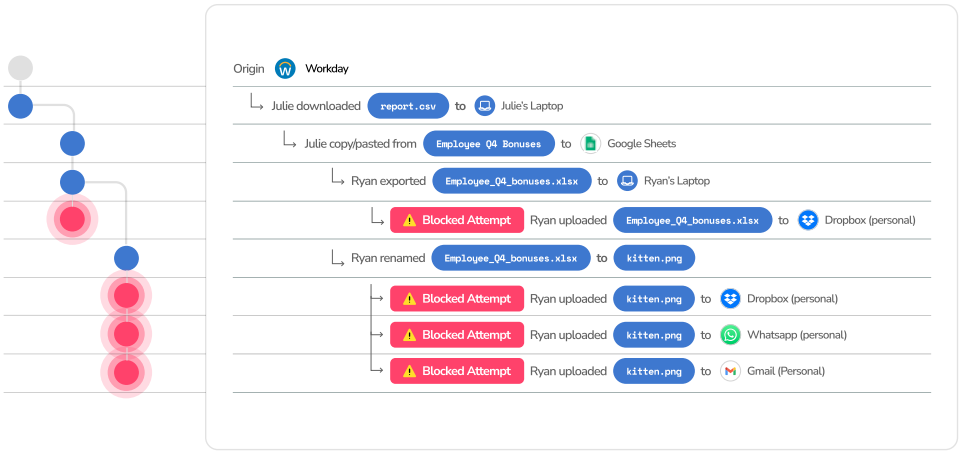
Whether you warn or block, Cyberhaven's end user popup messages are completely customizable — enabling real-time education that's more effective than messages and emails after-the-fact.

cyberhaven

4

Quickly investigate to understand user intent

Cyberhaven provides the full context of an incident to quickly investigate and respond to data leaks and insider threats.



Diagnose incident root cause

Cyberhaven provides analysts the complete history of events leading up to an incident in order to quickly understand the user's intent. We also show the full history of the piece of information, revealing how a user obtained data they don't have access to at the source.

Forensic evidence capture

Optionally, you can capture screenshots of a user's device in the seconds before an incident along with the offending file to better understand what happened. Both screenshots and files are stored by customers, not Cyberhaven.

Proactively monitor employees

Because Cyberhaven is always capturing every event for every piece of data, you can go back weeks or months and see what data an employee may have taken prior to submitting their two-weeks notice or regularly investigate specific employee groups that create and handle your most sensitive data.

cyberhaven

See our product in action

The best way to understand the magic of Cyberhaven is to see a live demo. Contact us at sales@cyberhaven.com to learn more.