cyberhaven

Data loss prevention reimagined

The limitations of traditional DLP

Traditional data loss prevention tools fail to protect important data, block normal activity, and use outdated technology that makes life painful for administrators and end users. We questioned every assumption and built a cloud-based DLP solution from the ground up to protect data in a better way.

Relies too much on content inspection

Relying entirely on content analysis, DLP tools don't accurately identify important data. They also generate false positive alerts that waste the time of analysts.

Creates a bad experience for end users

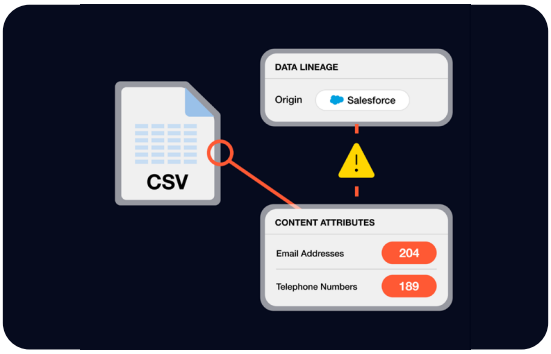
Because false positives block users from doing their work, the prevention features of DLP tools often aren't turned on. Their outdated technology also slows down computers and breaks cloud app.

Is time consuming to deploy and manage

Security teams need to invest a lot of time and resources fine tuning DLP content policies to reduce false positives. Older DLP tools also require on-premises software and databases.

Cyberhaven redefines data loss prevention

We identify important data that traditional DLP tools can't and protect that data across all exfiltration channels with one product and one policy.



Find, follow, and protect data that eludes content analysis

Important data often contains no recognizable content pattern, and sometimes no text at all. Data lineage helps us identify what other tools miss including:

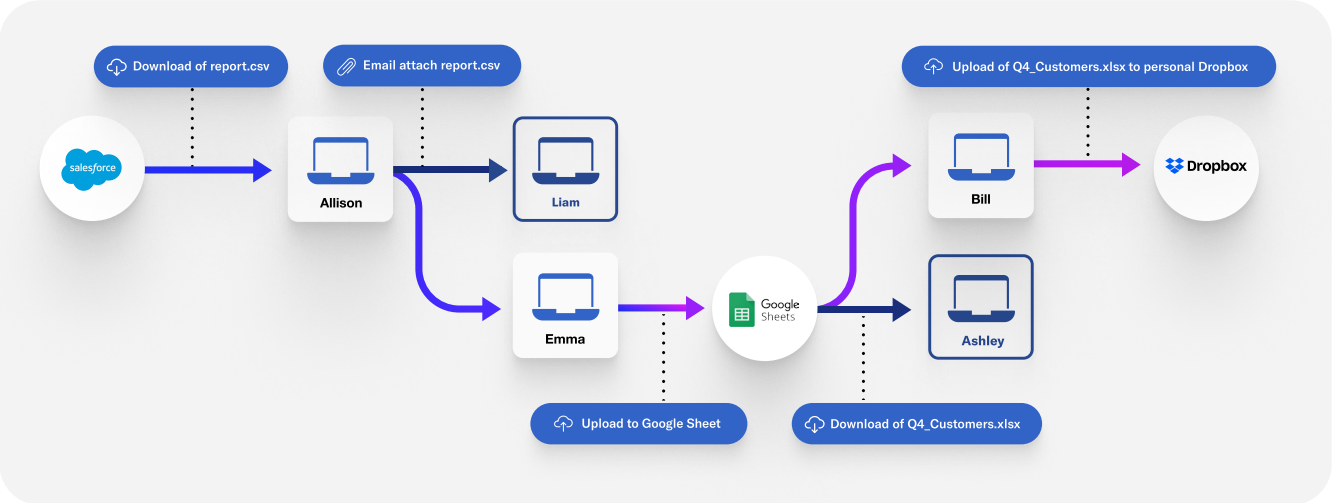
Combine content analysis and data

We combine content analysis with data lineage – where the data originated, where it's been, and who's handled it – to better identify what data is important and what's not. Our approach minimizes false positives created by common content patterns such as phone numbers and emails.

- **Client data**
- **Source code**
- **Product designs**
- **Financials**
- **Recorded meetings**
- **Employee HR data**
- **Architectural plans**
- **And more...**

The magic behind Cyberhaven is data lineage

Data lineage is a technology that's only available from Cyberhaven. It tracks data from its origin and everywhere it goes, providing the context we use to identify what data is important.



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

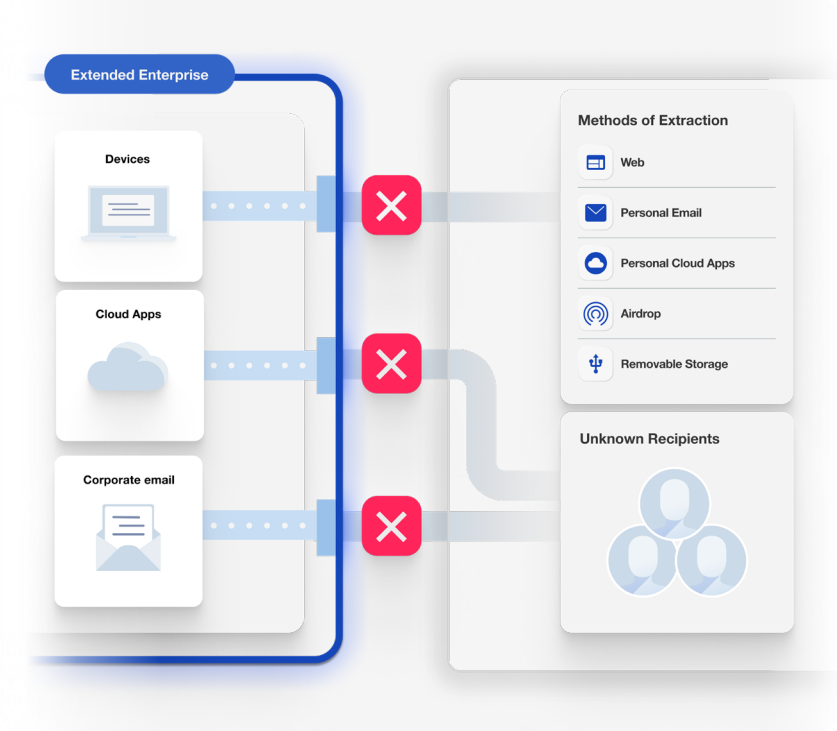
Data moves in recognizable ways, passing through the board meeting site in SharePoint or the employee offer letter account in DocuSign.

Who interacted with it

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

One product and one policy that protects all exfiltration channels

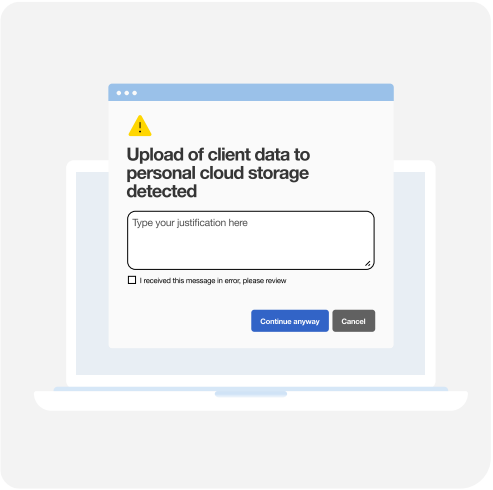
Cyberhaven prevents data in your extended enterprise from leaving your control with a single policy framework that applies everywhere your data goes.



Take real-time action to protect data and educate users on the right behavior

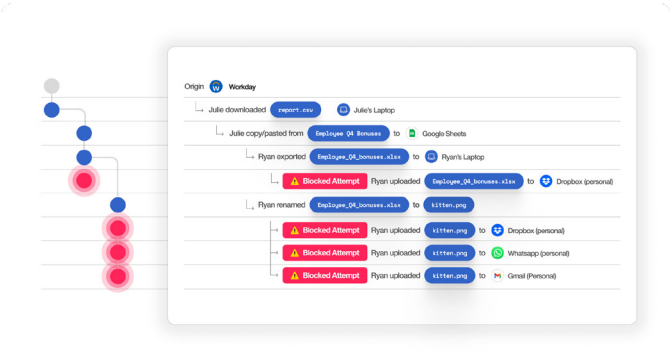
When data is at risk of being exfiltrated, instantly take action and surface a message to the user educating them on company policy and acceptable behavior. An educated employee base leads to 80% fewer incidents and reduced risk to data over time.

- **Block exfiltration of sensitive data**
- **Educate users to improve behavior**
- **Allow override with justification**



Investigate incidents with a full picture of the events before attempted exfiltration

Cyberhaven provides an incident response view tracing every step and action related to a piece of data leading up to an incident, including who handled it and how it moved throughout the organization so analysts can investigate and resolve incidents faster.



Simple, powerful policies that are easy to create and maintain

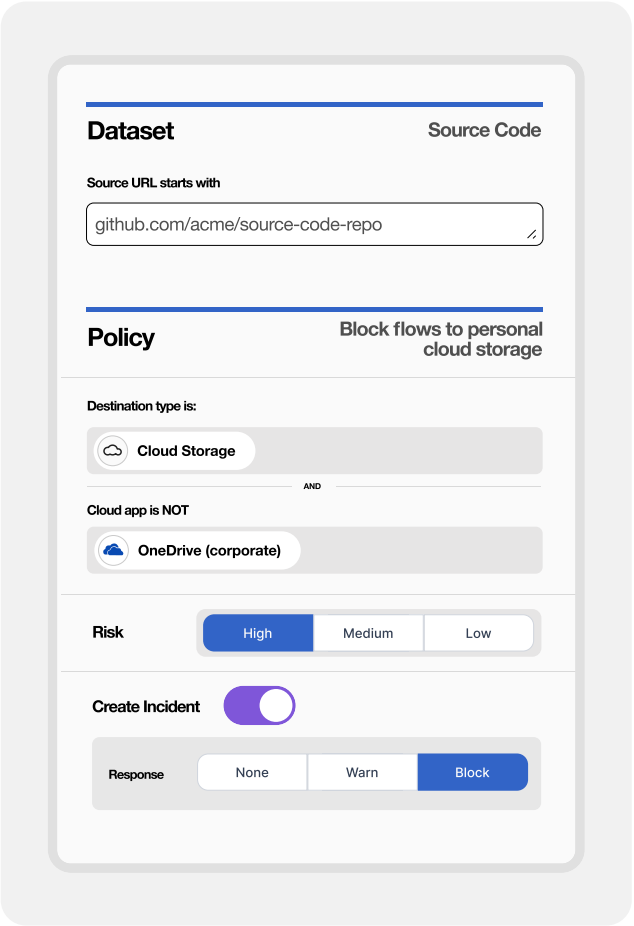
Cyberhaven data lineage makes it possible to define incredibly simple policies and get better results with fewer false positives than policies based on content analysis alone.

Define policies using an intuitive visual policy editor

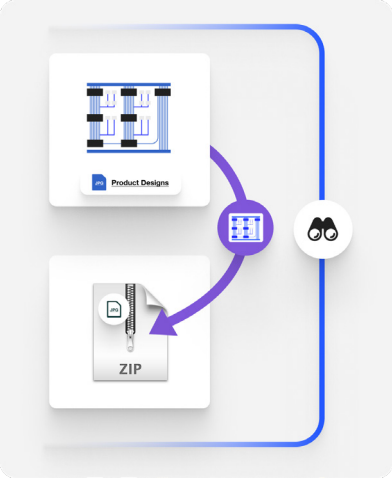
Cyberhaven data lineage makes it possible to define incredibly simple policies and get better results with fewer false positives than policies based on content analysis alone.

Test policies on historical data to quickly preview and iterate

Cyberhaven maintains a complete record of every user action for every piece of data. When editing a policy, you can see how it would apply to historical data to quickly make any adjustments without deploying it in production and waiting weeks for results.

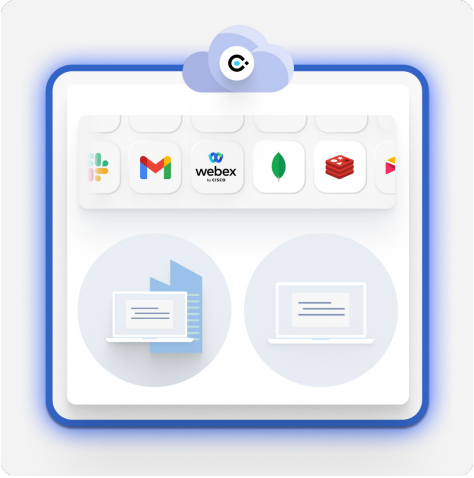


Protect data obscured by encryption and compression



Cyberhaven tracks what type of data was encrypted or compressed, so even after the data itself cannot be scanned you can track it and protect it from exfiltration.

Modern DLP delivered from the cloud



Cyberhaven's service is delivered from the cloud, so there are no databases or application servers to manage.

Everything else you expect from a DLP solution

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

Out-of-the-box policy templates

Get started quickly with dozens of out of the box policies for common use cases and industry-specific requirement.

Standard and custom content identifiers

Includes content identifiers for common PII, PCI, and PHI patterns, standard keyword lists, or create your own identifier with custom RegEx.

Recognizes third-party classification labels

Recognizes labels that classification products such as Microsoft AIP apply to files and supports labels in Cyberhaven policies.

Optical character recognition (OCR)

Extracts text content in image files and PDFs and supports use of this data in content-based policies.

Match highlighting

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

Screenshot capture

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

User directory integration

Integrates with on-premises and cloud-based directory services to support granular user group and department based policies.

Reporting and analytics

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

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.

Role-based access control

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

Go beyond DLP

Cyberhaven is more than a modern DLP solution, it's a new approach to protecting data from insider threats and accidental exposure we call Data Detection and Response.

The best way to understand the magic of Cyberhaven is to see a live demo.

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