SIMPLE RISK-BASED PROTECTION FOR ALL YOUR DATA, ANYWHERE IT GOES

Data is the heart of your business. Cyberhaven puts data at the heart of your security.

Organizations are defined by their data, yet for decades, data security has been complex, unreliable, and limited to only a few types of highly predictable data. Cyberhaven's Data Detection and Response (DDR) platform introduces a completely new approach that protects any type of data or intellectual property across its entire lifecycle, anywhere in the enterprise.

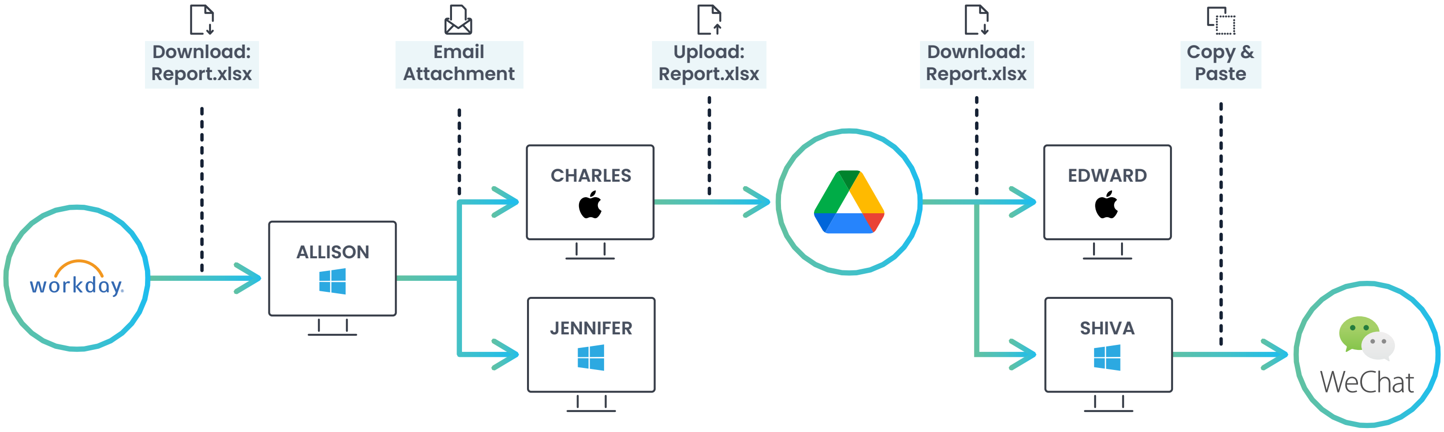
For the first time, security teams can support any business workflow across devices, applications, and cloud assets without ever losing visibility or control of the data. Simple policies automatically find and follow every copy of data - all without the need for complex rules, signatures, or pre-emptive tagging.

Cyberhaven's DDR Platform lets organizations protect:

- **Any Data** - Any data or intellectual property including PII, source code, design images, proprietary research, office documents, emails, etc.
- **Every Copy** - Automatically find and apply policy to every copy or derivative of sensitive data including data copy/pasted from one file to another.
- **Every Action** - Maintain context and control across every user action such as encryption, sharing over social media, use of personal cloud storage, and more.
- **Anywhere in the Enterprise** - Consistent visibility and control across endpoints, SaaS and cloud, file shares, USB drives, and more.
- **Safely and Simply** - Quickly define sensitive data based on origin or business context, and control risky behaviors without complex rules or tagging.

How DDR Works

Cyberhaven's DDR platform uses proprietary graph flow analysis known as Dynamic Data Tracing to automatically follow data as it's being used, moved, copied, transformed, or shared across the entire organization. A data trace includes the entire history (or lineage) of a piece of data and all its copies and derivatives, and looks like this:

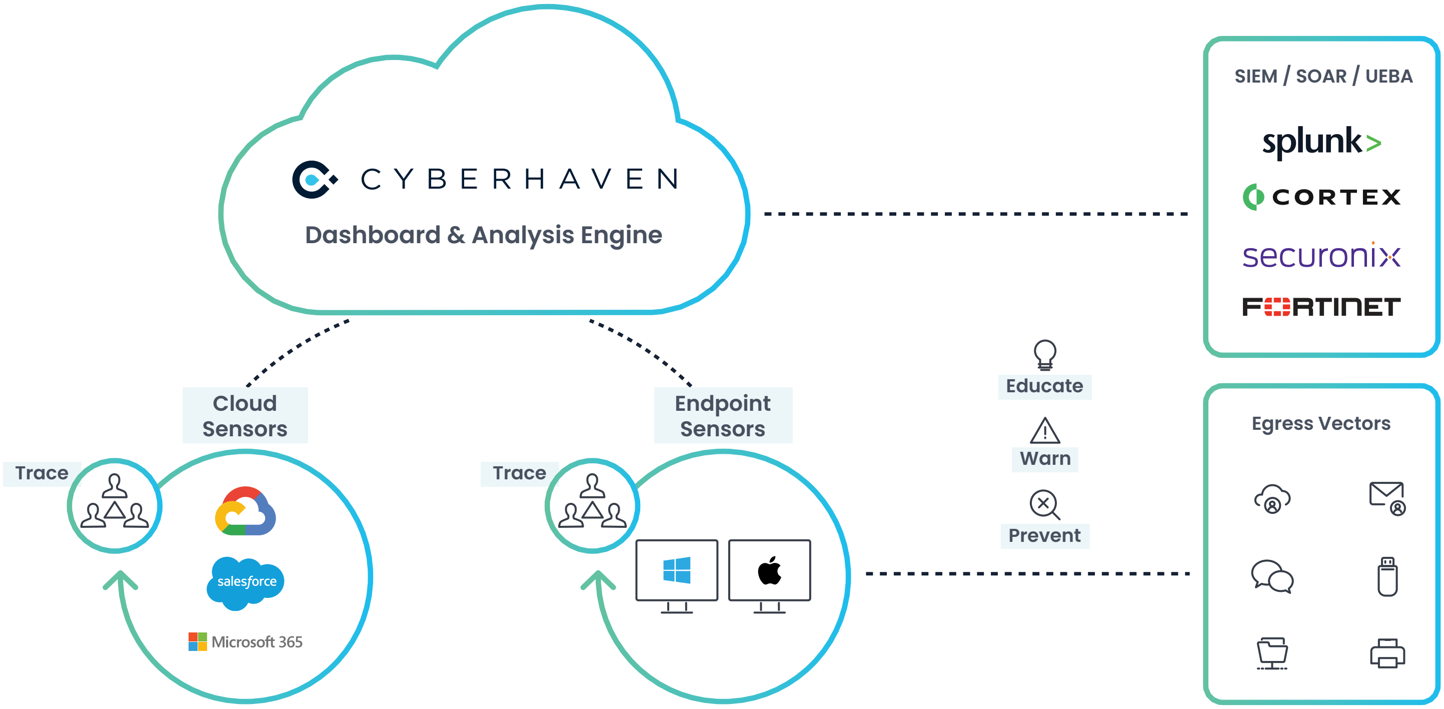


To build a data flow, Cyberhaven records and compiles low-level user and application data events from all monitored endpoints. The Cyberhaven analysis engine combines information from all hosts and uses proprietary graph analysis to link all events related to the same file into a single data flow. By seeing the full history, interconnection, and flow of all data, Cyberhaven can detect risks and enforce policies in a variety of ways:

- **Control any sensitive data based on provenance or origin** - Find numbers cut and pasted from spreadsheets, sentences copied from documents, Office documents exported to PDF files, etc.
- **Find and control snippets and derivatives of information** - Identify data cut and pasted from spreadsheets, sentences copied from documents, Office documents exported to PDF files, etc.
- **Assess privacy and security risks and enforce policy** - See all the systems where sensitive data are stored. Detect and prevent data from flowing to risky locations or moving in risky ways such as to social media, chat, or a user's personal cloud.

Cyberhaven Architecture

Each customer is deployed on a dedicated instance (SaaS service with a custom-built scalable graph database at its core) and all data in transit and at rest is encrypted by default. Through the endpoint and SaaS sensors, Cyberhaven records all data activity events and traces data to and from any emails, SaaS apps, network shares, and all data egress from endpoints (including shadow IT, encrypted communication, etc.). Cyberhaven was designed from the beginning to run in user space on both Mac and Windows, ensuring better performance for users (< 0.1% CPU usage), better stability and compatibility, and less work for IT and security teams.



With Cyberhaven, you are always in control of your data and always in control of your risk.