CYBERHAVEN CAN:

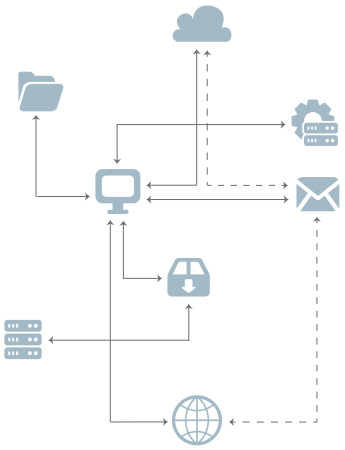
- **Completely automate data flow mapping**, requiring no input or effort from system operators or end users.
- **Trace end-to-end data flows** through all data silos and formats (like files, emails, IMs), from where data is created or enters the enterprise, across all on-premises and cloud locations, to leaving the enterprise.
- **Report in real-time** to keep data compliance accurate and up-to-date, because data tracing events are constantly being collected and mapped.
- **Alert your security team and end users** when data flows break your enterprise policies.

Automated Data Tracing

FOR MODERN DATA RISK MANAGEMENT AND COMPLIANCE

An increasing number of data privacy laws like GDPR, and frameworks such as NIST, HiTrust or ISO 27000 now make understanding and monitoring all data flows imperative. Regardless of format, structured or not, local or cloud, the need to know end-to-end data flows is essential but often remains a manual process or incomplete.

Cyberhaven offers a unique and simple solution to trace the flow of data through your entire enterprise in real-time. It is easy to implement and operate, and can be up-and-running in less than a day.



COMPREHENSIVE VISIBILITY INTO MOVING DATA

Data tracing is tracking and mapping the path of data and its derivatives into, across, and out of an enterprise. It is now mandated for compliance with many privacy laws but is equally important to protect data and prevent inadvertent data loss. Common applications include:

Map the paths of documents and files and their copies, for example showing the flow of a file containing intellectual property as it is copied out of the company's server to an employee's laptop, and then emailed to several recipients.

Document the journey of personal information, for example charting the path of information received from a customer by email, then cut and pasted into an instant message, then sent to an external system.

Understand data flows, for example diagramming the paths of all the documents and files that originated in a restricted folder to all their destinations.

CYBERHAVEN

Cyberhaven's Data Intelligence Platform continuously collects information on the movement of data from SaaS applications, cloud platforms and storage, email servers, and from on-premise systems and endpoints. This information is assembled in real time into interactive maps, graphs, and tables that answer a wide variety of questions about the movement of company's data. Analysts can observe big-picture patterns, or dig into every detail of data movement created by business processes, employee habits, or malicious activity by cybercriminals and rogue insiders.

The Data Intelligence Platform can be deployed within one day. There is no need to discover or categorize sensitive data in advance or to modify applications, systems, or networks.

> "When I first saw Cyberhaven in action, its real world value was instantly obvious."
>
> Adam Ely, Deputy CISO at Walmart

SIMPLIFIED COMPLIANCE, MODERN RISK MANAGEMENT, AND STREAMLINED SECURITY

The Cyberhaven Data Intelligence Platform helps enterprises comply with privacy and security regulations such as the European Union GDPR, HIPAA, PCI DSS, and the California Consumer Privacy Act of 2018, better manage data-related risks by applying cybersecurity and cyber risk frameworks such as NIST CSF, NIST SP 800-53, COBIT, and the ISO 27000 Series, and investigate and analyze security incidents.

CYBERHAVEN MAKES IT EASY FOR IT ORGANIZATIONS TO:

Comply with privacy regulations	Manage data risks	Investigate and report incidents
Automatically create data flow maps that demonstrate compliance with regulations and cyber risk frameworks. **Quickly and reliably find all copies of a specific customer's data**, in every email, document, and file, across all systems and platforms in the enterprise, SaaS applications, and cloud storage platforms. **Attribute all sensitive data to its origin,** for example tracing a snippet of data with customer information to an email from a customer, to a record in a SaaS application, or to a folder or database on the corporate network.	**Assess privacy and security risks**, by discovering all the systems where emails, documents, and files with data obtained from sensitive locations or containing sensitive attributes are stored, and determining if their security controls are appropriate. **Warn users to prevent them from violating policies,** for example by sending information obtained from customer A to customer B, or by storing documents with data obtained from sensitive locations on a cloud storage platform accessible to outsiders.	**Generate reports on what data was exposed during a breach**, for the CEO, board of directors, or regulators, by documenting which items were uploaded, emailed, or transmitted outside of the corporate network. **Investigate data leaks caused by breaches, insider threats, and user mistakes**, by mapping the data flows involved in the incident, pinpointing where data left the enterprise, and showing who moved the data – even when the data had not been identified as confidential prior to an incident.

Only the Cyberhaven Data Intelligence Platform provides a truly global view of data flows across the entire enterprise, including SaaS applications, cloud platforms, on-premises servers and storage systems, and employee endpoints such as desktop computers and laptops.

For more information, questions, or evaluation, contact us at info@cyberhaven.io