TRANSFORMATIVE DATA PROTECTION
With Dynamic Data Tracing

CYBERHAVEN

Cyberhaven protects high-value data throughout the data lifecycle while gaining insight into how that data is used and where it resides.

Re-Imagine DLP

Legacy DLP is a mainstay and necessary burden in most organizations for compliance. But what if data protection was always on for every piece of information your employees are creating as they communicate and innovate? Imagine that there was no need to tag or classify data.
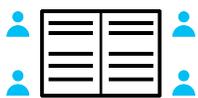
Top Challenges with DLP
2020 Survey by Cybersecurity Insiders

27%	Can't keep up with policies
25%	Limited data/file visibility
23%	Too many false positives
23%	Impedes productivity and collaboration
18%	Policies are too manual and complex

Data Tracing

Dynamic Data Tracing monitors all your data across on-premise and cloud environments, enabling you to to automatically detect the improper handling of your data without the hassle of tagging or classification. Cyberhaven extracts and records metadata from each user interaction with data so that you can inspect any data flow in real-time or retrospectively with just a few clicks. The result is effective data protection without impeding employee productivity and dramatically reduced incident investigation time and cost.

Key Benefits

Easily Monitor Movements for all Your Data

Immediately Detect Mishandling of Sensitive Data

Continuously Reduce Risk via In-Context User Training

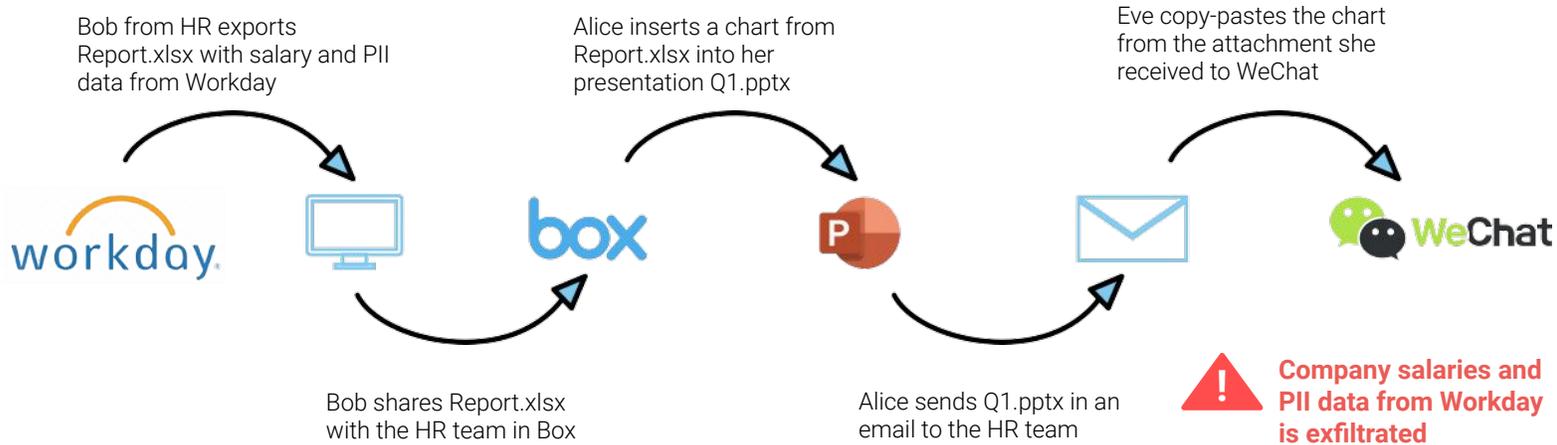Rapidly Investigate and Resolve Risk Exposure

IDA   **Deloitte.**   **motorola**   **WILLDAN**   **DARPA**   **SERVICESOURCE**

TRANSFORMATIVE DATA PROTECTION
With Dynamic Data Tracing

CYBERHAVEN

Data Tracing In Action: Journal of data lineage reveals business risk in an entirely new way.

Bob from HR exports Report.xlsx with salary and PII data from Workday

Alice inserts a chart from Report.xlsx into her presentation Q1.pptx

Eve copy-pastes the chart from the attachment she received to WeChat

Bob shares Report.xlsx with the HR team in Box

Alice sends Q1.pptx in an email to the HR team

Company salaries and PII data from Workday is exfiltrated

Data tracing reveals the whole story behind every piece of data

Cyberhaven uses endpoint and cloud sensors to trace data everywhere

Cyberhaven exposes the complete journey of data in simple intuitive flows that clearly identify mishandling of sensitive and regulated enterprise data. The following user activities are always recorded and continually analyzed for data risk events:

➔ Creation, upload, download, open, modify, move and copy
➔ Export of data and reports from databases and applications

➔ Cutting/pasting of content from emails, files and documents
➔ Sending and receiving email attachments

◆ Delivers comprehensive visibility by tracing all data activity automatically, across all data silos (including endpoints, email and an ever-growing number of SaaS applications).

◆ Creates a complete and contextual journal of how each piece of sensitive data was accessed and exposed.

◆ Visually highlights unexpected destinations for your sensitive data, to accelerate investigations.

◆ Educates users in real-time with configurable and escalating enforcement actions.

◆ Monitors sensitive data movements within cloud-based applications and platforms such as Office 365, SharePoint, G Suite, and Salesforce.

◆ Easily and rapidly deploy sensors and avoid data classification.

Contact us at info@cyberhaven.com