PROTECTING CREATIVITY FROM INSIDER THREATS

CYBERHAVEN

Security Threats in Media and Entertainment

M&E not only depends on a culture of collaboration but thrives on it. Collaboration drives creativity. In a recent Cybersecurity Insiders report, 42% of security practitioners cited collaboration apps as one of their main concerns, followed by cloud storage and file sharing apps. As a result, there are inherent conflicts with security and the collaboration culture that the M&E industry depends on for creativity. Collaboration opens the door for data leaks that immediately impact profits.

Data Behavior Analytics (DaBA) detects Insider Threats

Cyberhaven's new approach protects your creative ideas. Our Data Behavior Analytics (DaBA) solution monitors all data movement and user interactions, across multiple users and throughout on-premise and cloud environments. We immediately detect the improper handling of sensitive data by insiders in real-time. We can protect unstructured data such as designs, images and video. We can tell you who access a file, a database, a server and without classification track how the contents are shared, modified, and track all the locations where the content is stored. We can track how multiple users interact with the same data so that risky data sharing can be stopped.

Key Benefits
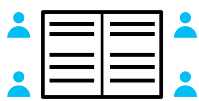
Easily Monitor Sensitive Data and User Interactions

Immediately Detect the Mishandling of Sensitive Data

Quickly Identify Risky Employees

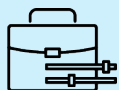**Rapidly Resolve Risk Exposure**

DaBA reveals the complete Data Journey

Continuous Data Monitoring across multiple users

Focus on interactions with sensitive content

Adapts to your way of doing business

Tracks all data everywhere

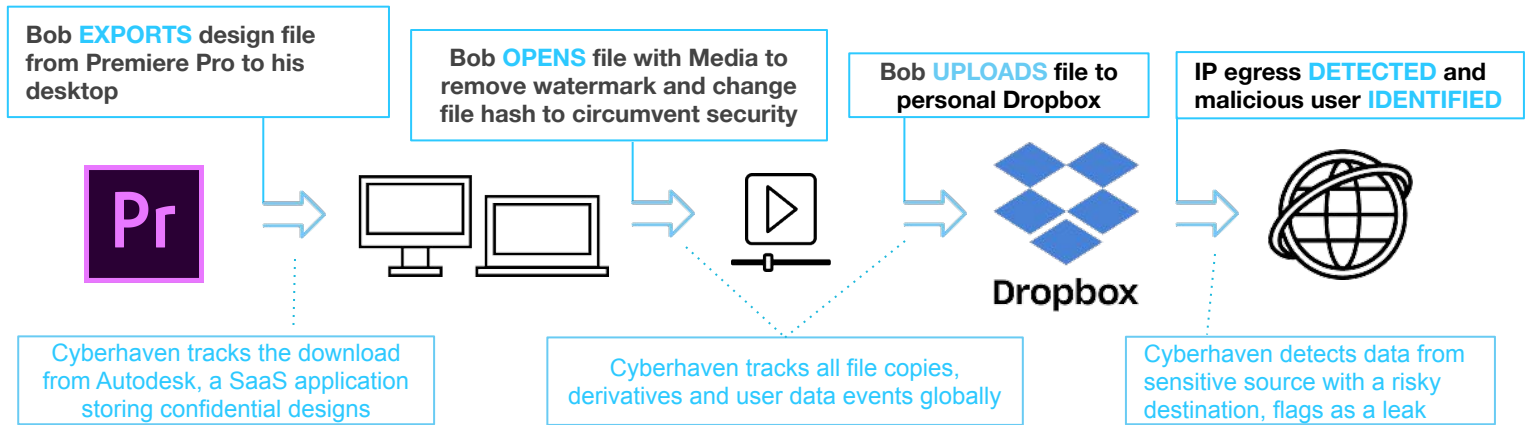Reduce risk with real-time response

IDA   Deloitte.   motorola   WILLDAN   DARPA   SERVICESOURCE

DaBA: MONITOR DATA & USERS

Data Behavior Analytics (DABA) in action: monitors the complete data journey including all user interactions to immediately reveal potential careless or malicious insider threats.

Bob EXPORTS design file from Premiere Pro to his desktop

Bob OPENS file with Media to remove watermark and change file hash to circumvent security

Bob UPLOADS file to personal Dropbox

IP egress DETECTED and malicious user IDENTIFIED

Cyberhaven tracks the download from Autodesk, a SaaS application storing confidential designs

Cyberhaven tracks all file copies, derivatives and user data events globally

Cyberhaven detects data from sensitive source with a risky destination, flags as a leak

Sensors trace data flows and journal all file activities including:

➔ 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

➔ Receipt of emails, files and documents

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

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

◆ Reveals the data journey of sensitive data highlighting surprising destinations.

◆ Tracks data behavior across all environments as data travels to and from cloud apps for insights into sources of risk.

◆ Monitors sensitive business transactions within cloud-based applications and platforms like **Office 365, SharePoint, and Salesforce**.

◆ Easy and rapid deployment of sensors gives immediate visibility.

Contact us at info@cyberhaven.com