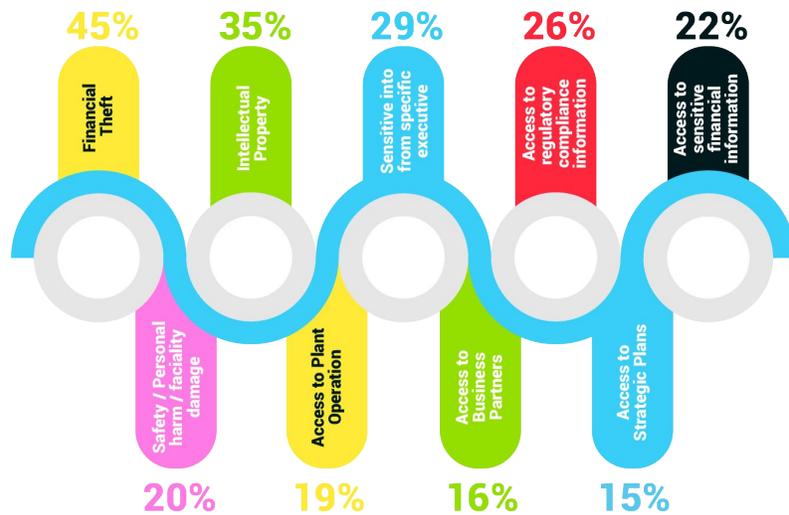# PROTECTING IP IN MANUFACTURING FROM INSIDER THREATS

CYBERHAVEN

SECURITY THREATS TO MANUFACTURING

The top concern for manufacturing is IP protection according to a Deloitte report. With ⅓ of budgets remaining flat there is insufficient funding to modernize and address security. Nearly 50% of manufacturing executives lack confidence that they are protected. More threats are coming from employees and there are rising concerns that manufacturing is increasingly at risk. Global instability increases employee fears of job loss and leads to unscrupulous behavior. Manufacturing needs to protect a variety of different data sources.

Top Motives For Cyber Incidents in Manufacturing Source: Deloitte

45% Financial Theft
35% Intellectual Property
29% Sensitive into from specific executive
26% Access to regulatory compliance information
22% Access to sensitive financial information

20% Safety / Personal harm / faciality damage
19% Access to Plant Operation
16% Access to Business Partners
15% Access to Strategic Plans

Data Behavior Analytics (DaBA) detects Insider Threats

Cyberhaven's new approach protects business critical data. It's **Data Behavior Analytics (DaBA)** solution provides complete visibility of the behavior and movement of all data (including trade secrets, intellectual property and sensitive data), across on-premise and cloud environments. It immediately detects the improper handling of sensitive data by insiders.

Key Benefits
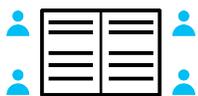
Easily Monitor Sensitive Data Movement

Immediately Detect the Mishandling of Sensitive Data

Quickly Identify Risky Employees

Rapidly Resolve Risk Exposure

IDA   Deloitte.   motorola   WILLDAN   DARPA   SERVICESOURCE
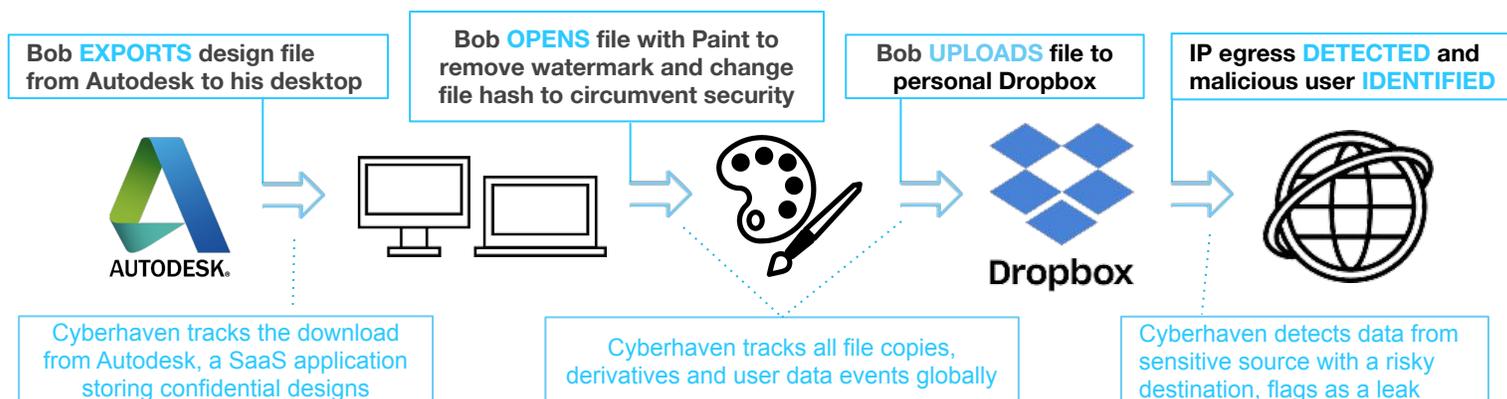
www.cyberhaven.com

INSTANT VISIBILITY WITH DaBA

CYBERHAVEN

Data Behavior Analytics (DABA) in action: links and shows the complete journey of data in simple intuitive data flows to immediately reveal the mishandling of data.

Bob **EXPORTS** design file from Autodesk to his desktop

Bob **OPENS** file with Paint 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