

# Incydr Data Security Assessment: Key Results

Prepared for [YOUR COMPANY]

## Welcome to a pivotal step towards strengthening your data risk landscape!

This assessment analyzes user activities, data destinations, and transfer vectors to pinpoint critical vulnerabilities in your organization's data exposure risks. Based on the findings, tailored recommendations are provided to enhance your data protection efforts.

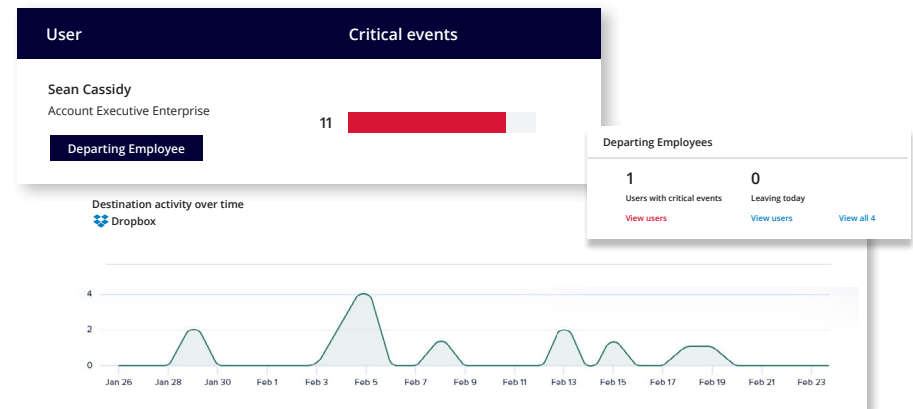
## Revealing Your Data Risks: A Ranking From Critical to Low Severity

### Risk Identified: Movement of confidential files to personal cloud drive

- **Risk Severity:** Critical
- **User:** Departing employee in the Sales department
- **File Details:** 5 customer lists were exported from Salesforce and uploaded to Dropbox

### Recommendations:

- Block unsanctioned uploads for departing employee user groups
- Prompt investigation when exfiltration occurs
- Escalate to manager, HR, and legal teams

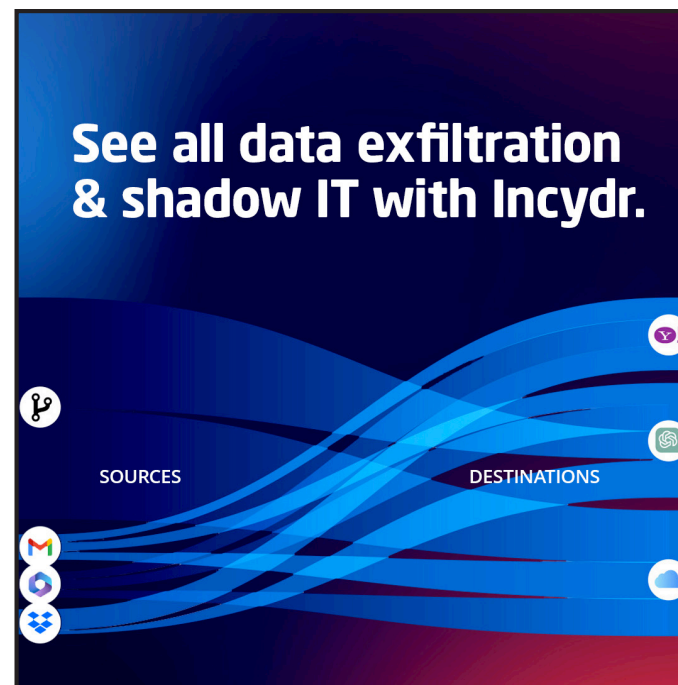


## Risk Identified: Push of proprietary **source code** to an unsanctioned repository

- **Risk Severity:** Critical
- **User:** Manager in the Engineering department
- **File Details:** 20 Python files uploaded to personal GitHub repository

### Recommendations:

- Enforce destination controls
- Initiate investigation with Incydr case
- Escalate to manager, HR, and legal teams



## Risk Identified: Web browser upload of financial data by an executive

- **Risk Severity:** Critical
- **User:** Executive team member in the Finance department
- **File Details:** 1 Excel file of financial data with an edited file name that suggests it's not sensitive data

### Recommendations:

- Implement automated alerts for web browser uploads
- Use end-user prompts for justification of actions

### MyCareerGoals.xlsx



Web browser upload (+4)  
High-risk employee (+2)  
Off hours (+1)  
**Risk score: 7**

**Date observed:** 2024-05-21 15:04:40 (UTC)  
**Vendor:** VMware  
**File path:** D:/

## Risk Identified: Unauthorized USB transfer by non-approved personnel

- **Risk Severity:** Moderate
- **User:** Specialist in the Marketing department
- **File Details:** 3 product roadmap documents

### Recommendations:

- Establish Acceptable Use Policy
- Deploy a security awareness training video (e.g., Mimecast Instructor)
- Block certain group of users, eg. repeat offenders, from the ability to use mountable media

#### ProductRoadmap.docx



Removable media (+6)

**Risk score: 6**

**Date observed:** 2024-05-10 15:04:40 (UTC)

**Vendor:** VMware

**File path:** D:/

## Recommendations for Long-Term Remediation:

- **Develop a holistic data protection strategy** that encompasses both preemptive measures and **ongoing security education** to foster a culture of data stewardship.
- **Implement behavior-based threat detection** with tools like Mimecast Incydr, ensuring comprehensive visibility across all endpoints and cloud services. This approach facilitates real-time, automated incident response, mitigating risks proactively.
- **Establish clear, enforceable policies** around **acceptable data handling** and device usage. Regular audits and policy reviews will ensure these guidelines evolve in line with new security challenges.



## Enhancing Your Data Risk Posture: Tips for Better Protection

Mimecast's analysis has revealed critical insights into your organization's data security posture, uncovering vulnerabilities that could potentially expose sensitive information to unwarranted risks. The highlighted concerns primarily involve unauthorized data transfers across various mediums — ranging from personal cloud storage to unsanctioned repositories.

### Mimecast: Trusted by Security and Preferred by Employees

Don't be the next company to hit headlines for a data breach. Our customers remediate massive insider incidents before major damage is done.

