

Incydr™ + Cloud Exfiltration Detectors




Detect and manage files shared from your Box, Google Drive, or OneDrive environment

Mimecast Incydr integrates with cloud storage services to detect and respond to improper sharing without impeding user productivity.

Integration Overview

Cloud storage services such as Box, Google Drive, and OneDrive allow employees to effectively collaborate with one another and are critical to how many organizations get work done. Incydr's integration with these services looks at all file activity across the corporate account. Unlike traditional security methods, this identifies any potential risk of files being shared and allows security practitioners to act quickly when there is real risk.

Features

-  **Full visibility**
Monitor Box, Google Drive, and OneDrive to detect public or unauthorized file sharing
-  **Access to file contents**
Gain temporary access to view file contents and assess risk
-  **Revoke shared files**
Admins can revoke access permissions when sensitive files have been shared with unauthorized recipients

Key Benefits

- **Data movement visibility**
Detect and respond when files are shared externally from your corporate Box, Google Drive, or OneDrive account
- **User & file context**
Quickly investigate exposure events using key details, such as who created the file, who has access to it, and the content it contains
- **Drive secure work habits**
Ensure appropriate use of Box, Google Drive, or OneDrive and oversee sharing with third party file sharing without disrupting legitimate work