CODE42

CODE42 INCYDR GOV FEDRAMP MODERATE AUTHORIZED

INCYDR

Data Risk Detection and Response for Insider Threat

Code42 Incydr™ Gov is a FedRAMP-authorized SaaS solution that proactively manages insider risk by protecting sensitive and strategic files from exfiltration. It brings together three dimensions of risk to quickly and accurately detect and respond to insider threat with unrivaled simplicity, signal and speed.

FILE

- Monitors all files – not just those that have been deemed sensitive
- Offers critical metadata including file name, owner, size, path, category and hash
- Provides authorized security analysts with the ability to review file content

VECTOR

- Detects exposure and exfiltration including web browser uploads, cloud sync app activity, Airdrop, and removable media
- Filters file events to reflect what is considered trusted vs untrusted activity
- Provides vector detail like sync username, domain name, browser tab title and URL, and removable media make, model, volume name, partition ID and serial number

USER

- Identifies behavioral Insider Risk Indicators such as remote activity, off-hour file events and attempts to conceal exfiltration
- Allows security teams to programmatically monitor users with increased risk factors, such as departing and contract employees
- Provides 90 days of historical user activity to surface trends and abnormalities

More collaboration, more insider risk.

Employees and contractors are being onboarded, enabled, empowered and offboarded, all in a remote world. Security teams need to keep up with these risks, while remaining compliant. Security tools like DLP, UEBA and CASB typically address a single dimension of risk, take months to deploy, and burden security teams with constant fine-tuning. It's time for a new approach to managing and mitigating data risk from insider threats.

89% of CISOs believe a fast-paced collaborative culture creates great risk

66% of data breaches involve an insider

69% of organizations breached by insider threat had a DLP solution in place

– Code42 Data Exposure Report

Incydr detects endpoint exfiltration events through vectors including USB, cloud sync applications, Airdrop, web browsers and other web apps.
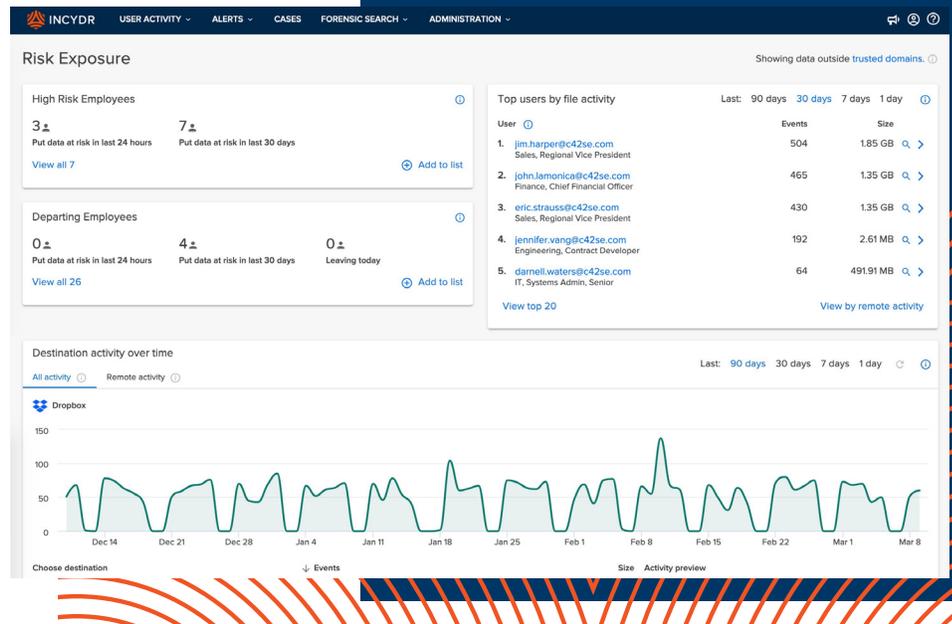

Detection: Pinpoint Insider Risk Indicators using dashboards, lenses and alerts.

Investigation: Simplify insider risk investigations with user profiles and forensic search.

Response: Integrate with SIEM, SOAR and other existing systems. Compile, document and disseminate evidence. Remediate risk through corrective or legal action, training, and more.

CODE42 QUICK FACTS

Founded in 2001

Locations:

Minneapolis (HQ) | Denver
Washington DC | London

Trusted by:

Customers include leading security brands such as CrowdStrike, Splunk, Ping Identity, Palantir and Okta

20 federal agencies across **8** departments

6 of **10** of the largest tech companies

13 of the world's most valuable brands

7 of **8** Ivy League schools

code42.com/gov

PRODUCT USE CASES

Remote workplace monitoring	Departing employee monitoring	High risk employee monitoring
Shadow IT detection	DLP policy validation	Improve security awarness
Contractor monitoring	Data Spillage/ Reclassification	Data exfiltration of sensitive files

FAST AND EASY DEPLOYMENT

- AWS cloud environment
- Windows, Mac and Linux
- 2-week average deployment time
- 230% ROI in 3 years
- Federal customer support based in U.S.