

# INTRODUCING CODE42 INCYDR



## Data Risk Detection and Response for Insider Risk

The Incydr™ SaaS product protects all of your valuable IP and strategic files such as source code, customer lists and product roadmaps without overwhelming security teams or inhibiting employee productivity. With unrivaled simplicity, signal and speed, Incydr brings together three dimensions of risk to quickly and accurately detect and respond to insider threat.



### 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 activity, file sharing, 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 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.

Organizations are moving faster than ever before. New IP is created every second, in the cloud using collaboration tools. Employees are being onboarded, enabled, empowered and offboarded, all in a remote world. Your security team needs to keep up with these risks, while remaining compliant, and enabling the business. 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 monitors file movement and sharing across computers, cloud and email using an agent and direct integrations.



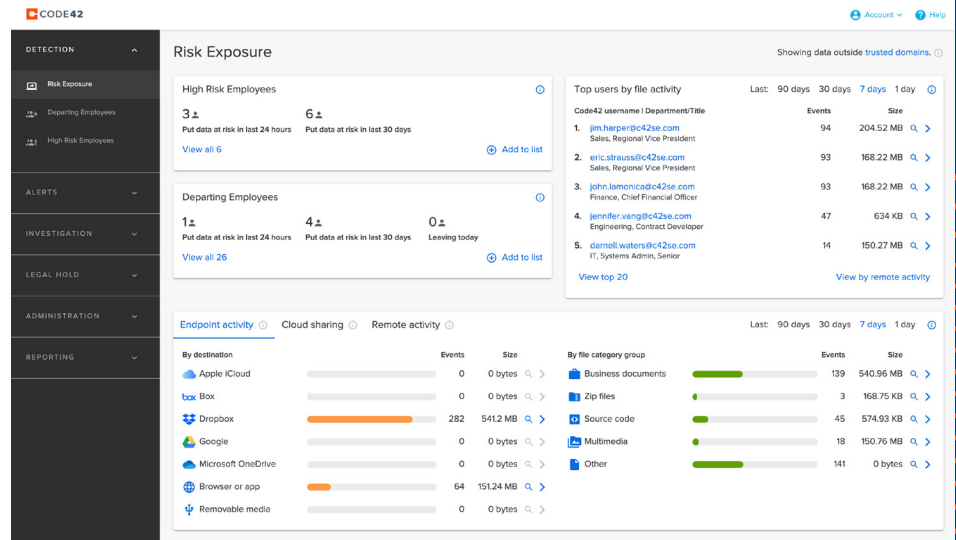
**Detection:** pinpoint data risk using dashboards, lenses and alerts



**Investigation:** simplify insider risk investigations with user profiles and forensic search



**Response:** compile, document and disseminate evidence. Remediate risk with SOAR playbooks, user conversation and training, legal action 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.

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

**13** of the world's most valuable brands

**7 of 8** Ivy League schools

## FAST AND EASY DEPLOYMENT

- Cloud-based
- Mac, Windows and Linux
- 2-week average deployment time
- 230% ROI in 3 years
- Customer support based out of US and UK

## WHAT OUR CUSTOMERS SAY

"If it wasn't for the Code42 ability to actually see the files, we wouldn't really understand what the person is doing... It provides us both speed and thoroughness of investigations."

— Tim Briggs, Director of Incident Response and eDiscovery at CrowdStrike

"It's crucial that we are able to detect and respond if employees are transferring data to personal accounts, or publicly sharing documents, especially when they depart. The Code42-Box integration gives us quick visibility into what is shared outside of our domain."

— Mark Campbell, Senior Director at Xactly

"Code42 is the only solution we have found that gives us the visibility we need to understand where data is moving, while still letting our team work how – and where – they need to."

— Dustin Fritz, Sr. Security Architect at UserTesting



Corporate Headquarters  
100 Washington Avenue South  
Minneapolis, MN 55401  
612.333.4242  
code42.com

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit [code42.com](https://code42.com), read [Code42's blog](#) or follow the company on [Twitter](#). © 2021 Code42. All trademarks property of their respective owners. (PO2009201)

# EMPLOYEE EDUCATION TAILOR MADE TO REDUCE INSIDER RISK

## CODE42 INSTRUCTOR

Code42 Instructor™ is Insider Risk reduction education that enables organizations to provide education to employees, where and when it's needed. Unlike traditional security awareness and education designed for general compliance and external threats, Code42 Instructor is employee education tailored for Insider Risk Management. Instructor focuses on what is needed to truly change user behavior and reduce Insider Risk by providing proactive organization-wide and department-level lessons, situation specific persona and technology lessons, and responsive user-specific lessons triggered by user activity.

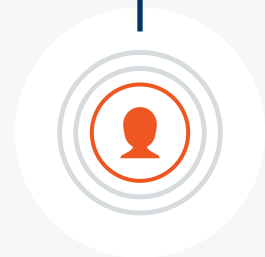
### Risk-based



### Real-time



### User-centric



### INSIDER RISK REDUCTION EDUCATION DESIGNED TO:

- Promote and ensure data use policy compliance
- Enable and empower a more risk-aware workforce
- Reduce accidental & negligent employee data leaks
- Measure, report and improve organization-wide Insider Risk posture

## PROACTIVE

Proactive Insider Risk lessons are compliance focused and culture minded meaning they are designed to empower employees to do the right thing and are SCORM ready to plug and play into any security awareness and training program.

### Proactive Instructor Lessons include:

- Insider Risk & You
- Keeping Source Code safe
- Keeping your Marketing data safe
- Keeping your Sales data safe
- Avoiding Common Data Risks: Google Drive edition
- Avoiding Common Data Risks with Slack
- Avoiding Common Data Risks: Office365/OneDrive edition
- Avoiding Common Data Risks with iCloud

## SITUATIONAL

Situational real-time Insider Risk lessons targeted for specific users or groups of users that are in the moment, engaging and relevant to the employee lifecycle.

### Situational Instructor Lessons include:

- Departing Employee: Dos-and-Don'ts
- New Employee: Dos-and-Don'ts
- Users with Elevated Access: Avoiding common data risks

## RESPONSIVE

Responsive Insider Risk lessons are user-focused to provide just-in-time training, user-friendly to deliver education in helpful, bite-sized chunks, and user-specific meaning they are triggered by unsafe user behavior or activity.

### Responsive Instructor Lessons include:

- iCloud sync
- Unsafe Personal Email use
- Google Drive - Unsafe Sharing
- Unsafe Slack use
- Office 365 - Unsafe Sharing

**Available in two packages, Instructor lessons are ready-to-use but also customizable.**

Learn more and preview Instructor Lessons [here](#).

## INSTRUCTOR

Best-in-class Insider Risk Reduction Training. Lessons tailored to help reduce Insider Risk proactively and responsively.

## INSTRUCTOR CUSTOM BRANDED

Custom branded Instructor lessons. Customize Instructor lessons with your company logo and information.



Corporate Headquarters  
100 Washington Avenue South  
Minneapolis, MN 55401  
612.333.4242  
[code42.com](http://code42.com)

Code42 is the Insider Risk Management leader. Native to the cloud, Code42 Incydr rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's Insider Risk solution is FedRAMP authorized and can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2021. For more information, visit [code42.com](http://code42.com). (P02109292)