Code42: Quick Reference Guide

Protect data from exposure, leak and theft caused by employees & contractors — whether malicious, negligent or accidental.

Code42 Products

code42 INCYDR

Code42 Incydr provides the visibility, context and control needed to stop data leak and theft. With Incydr companies can:

- Understand their risk
- Review what matters most
- Respond with confidence

code42 INSTRUCTOR

Code42 Instructor is user-friendly, automated, just-in-time and contextual security education focused on helping employees to:

- Become more risk-aware
- Reduce accidental & negligent data leaks

Instructor allows security teams to focus on high-priority alerts and real data exposure risks.

Economic Impact / Addressable Market

Average cost of just one insider risk data breach =

$4.6 million per incident

North American Commercial Total Addressable Market (TAM) =

$20 billion

What Makes Incydr Different?

- Access to exfiltrated files
- Unmatched browser upload detection
- Exfiltration detectors for corporate apps
- Context-driven prioritization via Insider Risk Indicators (IRI)
- “Trust model” to distinguish sanctioned vs unsanctioned apps
- “Right-sized” response controls
- Cross-platform agent

Ideal Customer Profile

Forward-thinking and progressive organizations that view people-collaboration and the associated intellectual property created to be of highest-value

Target verticals

- Technology | Software | Cloud
- Professional services | Consulting
- Manufacturing
- Fin-tech
- Biotech | Pharma | Medical Device
- Media & Entertainment

A Modern Approach

Code42 Incydr offers a modern approach to solving the data loss problem by providing the visibility, context & control to address data loss

Traditional DLP solutions restrict collaboration increasing workarounds and risk

CASB solutions provide limited visibility and may not cover endpoints

UEBA solutions establishes “normal” behaviors for the user but may trigger false alerts and doesn’t offer context

Security Education & Awareness solutions are commonly offered once or twice a year and content is quickly forgotten

Market Drivers

- Digital transformation and the advent of collaboration tools
- Employees working from anywhere
- People changing jobs faster than ever

code42

For additional information, visit the **Code42 Partner Portal** or **code42.com**

Code42: Quick Reference Guide

Protect data from exposure, leak and theft caused by employees & contractors — whether malicious, negligent or accidental.

Opportunity Spotters

- Departing employees
- Remote employees / contractors
- Recent IP theft / data breach
- Shadow IT
- Layoff & restructuring
- Mergers & acquisitions
- Sensitive, classified projects
- IPO

POV "Aha" moments

Compelling insights commonly surface during a standard Proof-Of-Value (POV) include:

- Source code exfiltrated to unsanctioned repositories
- Exfiltration of customer lists to personal email
- Salesforce report downloads to unsanctioned endpoints
- Public links to password files
- Sensitive IP renamed to mask exfiltration

Questions To Ask Your Prospects

What is your **strategy to protect your data**? Is it working? Why? Why not? If it's not working **what kind of impact** does that have on your business?

What "blind spots" do you have related to where your **sensitive data and IP** is and **how it is being used by employees**?

What concerns do you have about your a**bility to detect and respond to files leaving your organization**?

What processes do you have in place to **protect your data when someone leaves your company**?

What is the **most important IP** in your company? What types of groups or users have access to more of your **high-value data**?

What percentage of your workforce **works from home or off network**? How does this impact your **visibility into their file activity**?

Gartner Reviews

Gartner peerinsights.

Code42 Customer reviews

Customer Success Stories

Okta Chooses Incydr Over CASB to Avoid Data Leak from Cloud File Sharing

How Snowflake Keeps Critial IP Safe Without Disrupting Productivity

Lyft Uses Incydr to "Take the Blinders Off" of High-Value Data Movement

More Code42 Customer Success Stories

Fast Time to Value

Companies are able to deploy Incydr in hours and be fully operational in days. For example:

- 90 agents silently deployed to endpoints within first hour of POV
- 15,000 endpoints deployed per week

Technology Partners

- Palo Alto Networks
- Okta
- Rapid7
- CyberArk
- Tines
- Splunk

code42

For additional information, visit the **Code42 Partner Portal** or **code42.com**