CODE42

HOW INCYDR WORKS:

A TECHNICAL OVERVIEW OF THE INCYDR PRODUCT ARCHITECTURE

INCYDR

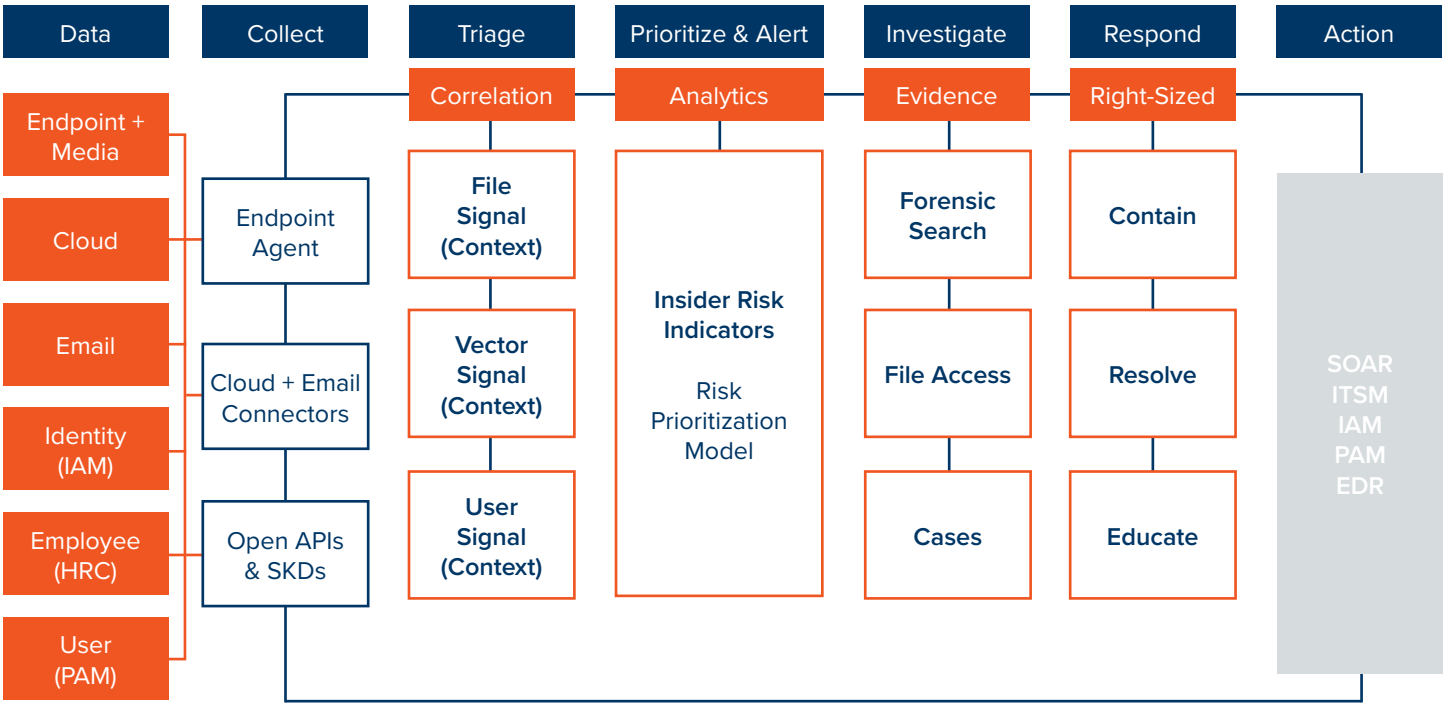
Incydr is the purpose-built solution to manage Insider Risk. Its approach to data protection is rooted in simplicity, signal and speed. This overview outlines Incydr's product architecture and explains how it meets Insider Risk Management requirements.

ARCHITECTURE OVERVIEW

Incydr is a SaaS data risk detection and response product. It leverages an endpoint agent and API integrations to monitor file activity and detect Insider Risk. It can be deployed in hours to provide an understanding of organization-wide data exposure in days.

Incydr's agent and integrations send file, vector and user information on detected events to the Code42 cloud to power Incydr's detection, investigation and response capabilities.

Incydr Architecture



Incydr Architecture

Endpoint
Agent

- Non-disruptive to employee productivity
- File + Vector + User monitoring
- Mac, Windows, Linux support

SaaS
Console

- Company-wide and per user visibility
- Assess organization-wide risk in < 2 weeks
- Improve organization risk posture in < 3 months

API
Integrations

- Monitor for data risk events in corporate cloud and email systems
- Steamline processes & workflows via HRC, ITSM
- Right-size response via IAM, SOAR and more

ENDPOINT AGENT

Incydr's agent is installed on desktop and laptop computers. It runs on Windows, Mac and Linux operating systems. The agent is used to detect file events. A file event is defined as file creation, modification, deletion or movement. Incydr labels events as exposure events when files are transferred to removable media devices, uploaded to browsers, or accessed by monitored installed applications. The agent securely sends event details, file metadata and, for exposure events, the file itself to Code42 cloud destinations to be indexed and analyzed. This information is made available to the administrator via the web console within 20 minutes of the event. By storing this information in the cloud, administrators are able to view, query and interact with this data without impacting device performance, and regardless of whether the device is currently online. This data is retained for 30 or 90 days, depending on the subscription purchased.

During implementation, the agent is configured to monitor a set of files and applications. It monitors files located on the primary disk which is C:\ on Windows and / on Mac and Linux. Watched applications are those used to transfer files from a device. This includes web browsers (e.g. Chrome, Firefox, Edge), cloud sync applications (e.g. DropBox, iCloud, Google Drive), Slack, Airdrop, sFTP, Curl and others. Administrators can add custom applications to be watched. The agent registers with the operating system to be notified about file activity. The agent is notified when a file event occurs within a watched path or application. The agent has secondary scanning technology to scan for any events that might occur when this notification would

QUICK FACTS

- **The agent is used to detect file events on Windows, Mac and Linux computers.**
- **It securely sends event details, file metadata and file contents to Code42 cloud destinations to be indexed and analyzed.**
- **The agent is configured to monitor a set of files and applications.**
- **Information is extracted from detected file events and sent to the cloud for secure storage every 5 minutes.**
- **By storing this information in the cloud, administrators are able to view, query and interact with this data without impacting device performance, and regardless of whether the device is currently online.**

not take place, such as during device startup or shutdown.

Metadata and event information (discussed later in this paper) is extracted from all detected file events. Detected events are added to an event report. These reports are sent to a secure cloud environment every five minutes. If the device is offline, the event reports are sent when the device reconnects to the internet.

API TO API INTEGRATIONS WITH CLOUD SOLUTIONS

Incydr connects with other security and business systems through API integrations. These systems are used as data inputs, outputs or both.

Cloud Connector Integrations

Incydr connects with corporate cloud and email systems to detect file exposure and sharing events. These include Gmail and Office365 for email, and GoogleDrive, OneDrive and Box for cloud storage and sharing. The role of these integrations is to allow Incydr to detect when files are made publicly available or shared with untrusted recipients via corporate systems.

Administrators must authorize Code42 as a registered client API using their administrator account.

Cloud Collaboration Platforms

- Once authorized, Incydr monitors for file events such as sharing and permission changes. It receives this information directly from the cloud platform within 5 minutes of an event.
- Incydr parses the file, user and vector metadata on every cloud event. It stores this information for correlation, visualization, alerting, and search within 20 minutes of the activity.

Corporate Email Solutions

- Once authorized, Incydr monitors for emails that are sent with attachments. This allows it to detect when files are sent to untrusted or external users. It receives this information directly from the cloud platform within 5 minutes of an event.
- Incydr parses the file, user and vector metadata on every email event. It stores this information for correlation, visualization, alerting, and search within 20 minutes of the activity.

Workflow Automation Integrations

Code42's workflow automation integrations enable security teams to customize and automate Insider Risk processes. Code42's professional services team creates and maintains automations for more than 400+ data connections including Okta, Workday, ServiceNow and Slack.

These integrations are no-code workflows. Customer administrators authorize an API connection to a company's chosen system, and Code42 professional services team builds an automated workflow according to Code42 Insider Risk Management best practices and the customer's preferred process.

Example workflows include:

Right-Sized Response workflows
Use Incydr alerts to trigger a change in a user's access permissions within Okta. Connect Incydr to Slack to perform streamlined user outreach by leveraging pre-populated direct message templates with event information.

Insider Risk Indicator workflows
Connect with an HR platform such as Workday, ADP or Bamboo HR to ensure Incydr automatically receives the departure date information for departing employees in order to detect this Insider Risk Indicator (IRI).

DIFFERENTIATORS OF INCYDR'S APPROACH

A Comprehensive Record of All File Activity

Incydr provides the ability to investigate any file exfiltration event. This is due to the fact that it detects and logs all file activity. Administrators do not need to define policies for what should be monitored and logged. Although Incydr records all employee file activity, and makes it searchable for investigation, it only visualizes and alerts you to the events that indicate Insider Risk. This ensures signal, not noise.

In addition to being more comprehensive, Incydr's approach to monitoring is also less burdensome. By monitoring everything, there is no need to create and fine-tune policies. And because of how the agent and cloud integrations monitor events, there are no proxies, SSL inspection or browser plugins to configure and maintain.

QUICK FACTS

- **Incydr has API-based integrations with a wide range of cloud systems.**
- **This provides unified visibility across corporate computers and systems.**
- **There are no proxies, SSL inspection or browser plugins to configure and maintain.**
- **Incydr monitors file activity within cloud and email systems to detect high-risk events such as unauthorized file sharing. This activity is indexed and stored just like a user's endpoint activity. This ensures Incydr detects and prioritizes all Insider Risk, no matter where that risk occurred.**
- **Incydr connects with IAM, HCM and other corporate systems to automate Right-Sized Response and Insider Risk Indicator workflows.**

Insider Risk Prioritization that's Context-Driven, Pragmatic and Adaptable

Incydr prioritizes your highest risk users and events so you can clearly differentiate between harmless file movement and data leak or theft. Notably, Incydr is even able to distinguish between personal and corporate activity when the same service is used for both purposes (example: personal Gmail and corporate Gmail). We call this increasingly common risk Mirror IT.

When monitoring all file activity, Incydr watches for Insider Risk Indicators (IRIs). IRIs are activities or characteristics that suggest corporate data is at a higher risk of exposure or exfiltration. They are used to prioritize the greatest risk to the organization.

Incydr's extensive library of IRIs is categorized by file, vector and user risk indicators. Incydr assigns a numerical risk score to every IRI. These scores are totaled to determine the overall risk of a detected event. The risk score of an event determines the event's severity. Events are prioritized by severity, and users are prioritized by the number of critical events they trigger. This method of prioritization allows Incydr and security teams to take a use-case driven approach to Insider Risk Management.

If needed, Incydr administrators can adjust the default severities to fit their own risk tolerance. Risk settings allow administrators to adjust these risk scores and modify how users and events are prioritized. Trust settings tell Incydr what activity it should de-prioritize. This prevents approved file activity from triggering alerts or cluttering dashboard views.

Below are examples of how Incydr prioritizes Insider Risk events. Remember, all defaults can be tuned to your risk tolerance. For example, Incydr does not assign a risk score to video files by default. However, if you run a production studio where video files comprise much of your intellectual property, you can increase their risk score.

= **16, Critical Severity**

A **departing employee** sends a **zip file** using **ProtonMail**.

= **12, Critical Severity**

A **contract employee** sends a **zip file** to **Airdrop** during **off hours**.

= **8, High Severity**

An **employee** uploads **source code** to **Dropbox**.

= **4, Moderate Severity**

An employee with **poor security practices shares a video file** in **OneDrive to an untrusted domain**.

= **3, Low Severity**

An **employee sends a video** to a **personal Gmail address**.

Accurate Investigation Context

When it comes to Insider Risk, context is everything. Incydr ingests and correlates all the context you need to make informed investigation decisions. Below is a sample list of some of the forensic metadata Incydr offers.

Filename	**Risk Indicators**	**Hostname**	**Bus Type**	**Executable Name**
File Path	**Date Observed**	**Fully Qualified Domain Name (FQDN)**	**Capacity**	**Tab/Window Title**
File Category	**Event Type**	**Username (Code42)**	**Vendor Name**	**Tab URL**
File Size	**Source**	**Username (signed into device)**	**Device Name**	**Sync Destination**
File Owner	**Process User**	**IP Address (public)**	**Device Media Name**	**Sync Username**
MD5 Hash	**Trusted Activity**	**IP Address (private)**	**Device Volume Name**	**User Role and Department**
SHA256 Hash	**Exposure Type**		**Device Partition ID**	**User's Active Hours**
File Created Date	**Destination Category**		**Serial Number**	**User Activity History**
File Modified Date	**Destination Name**			

Incydr also allows authorized security administrators the ability to access and review file contents during investigation. This enables you to verify the accuracy of anything Incydr flags as a risk. It also enables you to validate instances where files are obscured to look like something else. This is referred to as a File Mismatch IRI. An example is a 2022_Roadmap.pptx masquerading as HawaiiVacation.jpg.

Right-Sized Response

Insider Risk is dynamic, so response must be driven by event context and severity. There's no one-size-fits-all Insider Risk action. A range of human and technical responses are needed.

Incydr enables right-sized Insider Risk response:

- **Efficiently perform and document investigations**
- **Automate technical containment controls**
- **Accelerate resolution**
- **Improve security awareness and posture**

Incydr Response Best Practices

Response Type	Contain	Resolve	Educate
Purpose	Stop ongoing data exposure	Remediate detected data exposure	Reduce future data exposure
Controls	• Reduce access permissions • Remove system access • Stop local sync apps • Disable USB port • Network contain endpoint • Lock device	• User inquiry • Resolve over screenshare • Attestation of deletion • Manager escalation • HR escalation • Legal escalation	• Acceptable Use policy • Monitoring message at endpoint startup • Send policy reminder • Training assignment
Trigger	Critical severity events	Critical and High severity events	Ongoing/as needed

It's important to note that these response types are not sequential steps nor are they mutually exclusive. Organizations can respond with one or more response types (contain, resolve, educate) depending on an event's severity and their own risk tolerance. These controls are available through Incydr automations and integrations with systems such as SOAR, IAM and EDR.

To formalize insider threat investigations, Incydr's Cases feature provides you with an efficient way to compile, document and disseminate investigation summaries. Security team members can add data exposure events to a case from within Forensic Search. This documents and retains the data exposure event details indefinitely. Within a case, you can reference important user context and summarize findings and recommendations from your investigation. Cases can be quickly exported and sent to business stakeholders like management, legal and HR.

The Market Standard for Insider Risk Management

Incydr offers a context-driven approach to prioritize risk, contain data exposure, accelerate resolution, and educate users on appropriate data handling. Ultimately, security teams who utilize Incydr are able to avoid corporate data leak and drive the behavioral change needed to improve their Insider Risk posture.

Incydr supports the 5 stages of the Code42 Insider Risk Management framework so security teams:

- Know where, when and how data is exposed, and by whom
- Know what activity is trusted vs untrusted
- Know when data is most at risk
- Know how to respond
- Know if their Insider Risk Management strategy is working

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, and Okta

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

13 of the world's most valuable brands

Gartner Peer Insights

35+ Verified Security Reviews

★★★★★

4.9 out of 5 stars

Code42.com

FAST AND EASY DEPLOYMENT

- Mac, Windows and Linux
- 2-week average deployment time
- 230% ROI in 3 years
- Agent on endpoint can be deployed silently

WHAT OUR CUSTOMERS SAY

"Once deployed, this is an immediate data loss detection solution. I would not need someone to keep the rules up to data. The dashboard is simple and anyone can identify where to review without much training."

CROWDSTRIKE

- **Tim Briggs**, Director of incident Response and eDiscovery at CrowdStrike

"When we looked at solutions like the more traditional DLP or the CASBs, it seemed like they work under very limited conditions. But, the minute you put them out in the real world, they just break down. Without hesitation, Incydr... is central to our security program."

snowflake

- **Mario Duarte**, VP of Security at Snowflake

"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."

UserTesting

- **Dustin Fritiz**, Sr. Security Architect at UserTesting

CODE42

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, read Code42's blog or follow the company on Twitter. (WP2105263)