Insider Risk Management Framework: A Better Way to Prevent Data Leaks with Code42

One year ago, an abrupt influx in remote work and collaboration tools changed the way we work, dare I say forever. With that came increased risks to company data — employees are 85% more likely to leak files today than they were pre-Covid, according to the 2021 Data Exposure Report. This data risk problem is the elephant in the room. Trailblazers like Rakuten are doing something about it — are you?

Why It's Time to Take an Insider Risk Management Approach to Data Protection

The first step to solving a problem is naming it, and this one is called Insider Risk. Insider Risk is any data exposure event — security, compliance or competitive in nature — that jeopardizes the financial, reputational or operational well-being of a company and its employees, customers and partners. While this may sound like a marketing buzzword for insider threat, it is not. The distinction is that insider threat puts a magnifying glass on the employee, and insider threat tools like UEBA take a user-centric approach. Insider Risk Management solutions go beyond this by taking a data-centric approach that combines the three dimensions of risk — files, vectors and users.

Code42's Insider Risk Management (IRM) framework provides a 5-stage practical guide, complete with technology and integration requirements needed to deter Insider Risk. The rollout of Code42's IRM framework comes on the heels of Code42's designation as a Representative Vendor in the December 2020 Gartner "Market Guide for Insider Risk Management Solutions" report. Code42 Insider Risk Management is the solution for protecting data from insiders while ensuring compliance with data use policies, creating a more risk-aware culture and accelerating security's time to value. Our approach is actualized through the technology we build, services we offer and partners we integrate with. We deliver on this promise with a foundation built on three core pillars:

1. Monitor all files, vectors & users

All data is important. Compliance-driven approaches that depend on classification and policies create blindspots that miss the everyday data risk — from valuable data that is classified inaccurately, emerging exfiltration vectors that policies did not anticipate or non-malicious employees just doing their jobs.

2. 100% Cloud-native

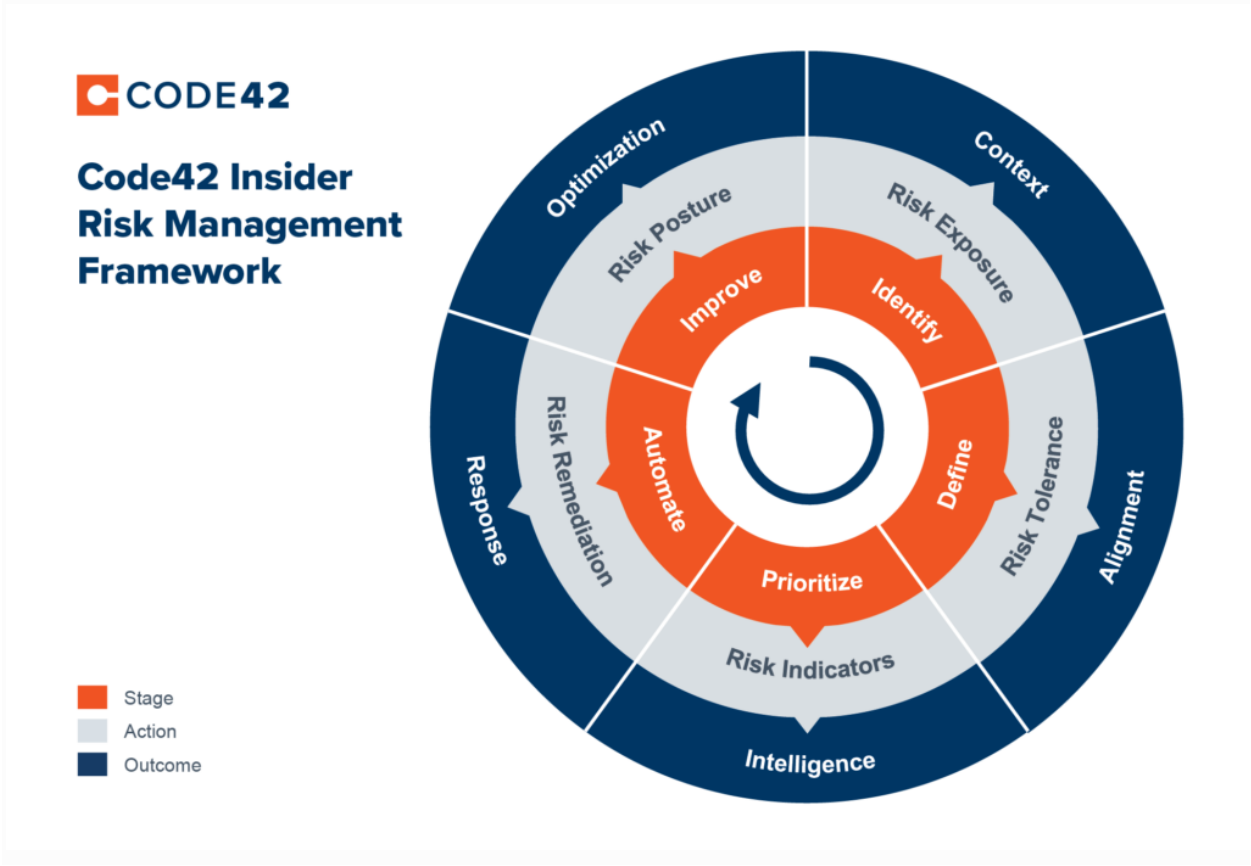
Our dispersed workforce isn't going away anytime soon. To keep pace and speed the time to value, security teams need to invest in solutions that don't require on-premises hardware or networks. Employees are adopting cloud collaboration tools and platforms at an exponential rate, making it imperative that security teams have the capabilities needed to protect data as it traverses between the endpoint and cloud applications.

3. Non-disruptive to employee productivity or collaboration

Employees willingly and unwillingly expose or exfiltrate corporate data every day. Knowing the distinction between malicious intent and collaboration, followed by a response that is right-sized for the situation is the holy grail of Insider Risk Management. Our IRM framework provides the technical recommendations necessary to help analysts and architects machine their intuition in order to prevent data leaks, not collaboration.

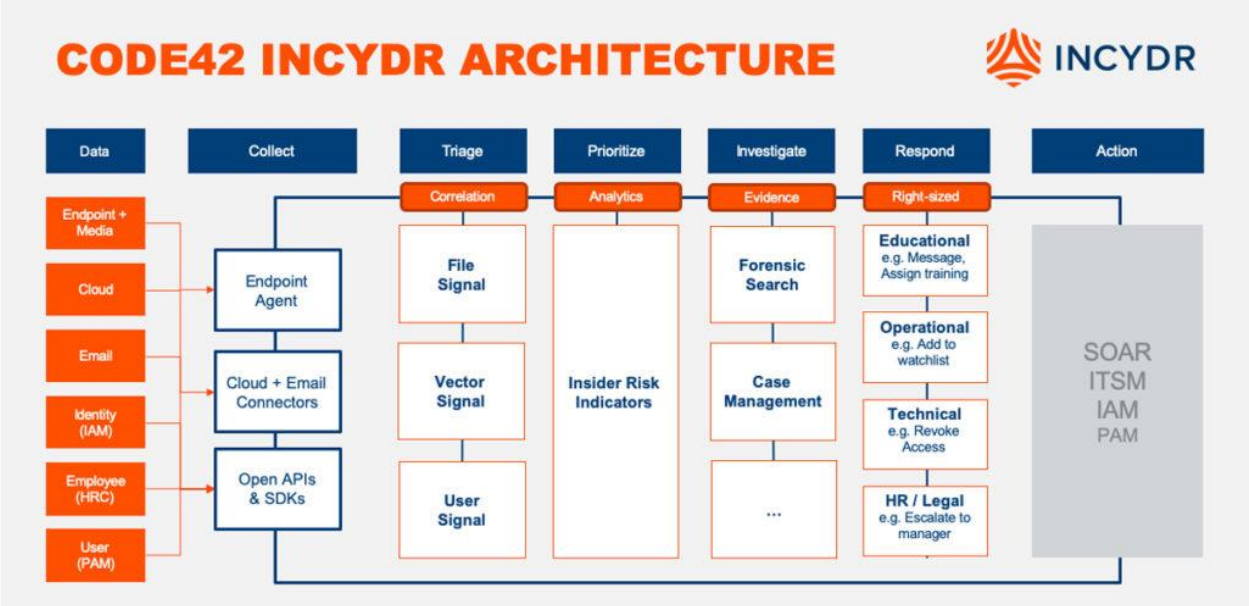
Making an Impact with a Purpose-Built IRM Solution

Instead of a mere perception of protection that conventional DLP approaches create, an IRM approach to data protection prioritizes the tangible realization of value through measurable Insider Risk reduction. To help security teams accomplish this, Code42 has developed a pragmatic and realistic framework rooted in five core technical requirements.



1. Identify: It is crucial to have IRM technology in place that can monitor and identify the three dimensions of risk – file, vector and user – across all data, and is environment (Windows, Mac, Linux) agnostic.
2. Define: Security teams must define trusted versus untrusted activities, scenarios and risk indicator severity to align on organization-wide Insider Risk tolerance and right-sized response.
3. Prioritize: It is crucial that IRM technology can triangulate individual aspects of file, vector and user context to surface leading indicators of risk. This capability allows risk that comes with source code exfiltration, suspicious file type mismatches, syncs to personal cloud storage and departing employees to be surfaced above lower severity events.
4. Automate: Automate a combination of human and technical actions to accelerate Insider Risk response. Because not all Insider Risk is malicious, response actions should be right-sized to the risk severity and situational context.
5. Improve: Measure and optimize the organization's overall Insider Risk posture and maturity by improving technology implementation and processes over time.

Code42 Incydr is the purpose-built solution for Insider Risk Management. We know that every organization's tech stack and data risk priorities are unique, but you can expect that architecting Incydr as a solution for Insider Risk Management may look similar to this.



We published the Insider Risk Management Framework, built the technology, and wrote the book on Insider Risk. Gartner published the Market Guide for Insider Risk Management Solutions. Trailblazers like Rakuten and Snowflake are paving the way as early adopters of a new approach. We are ready to help you get started on our journey to managing Insider Risk. To learn more about Code42 Incydr, please visit https://www.code42.com/product/.