Insider Risk Management – A Better Way

to Prevent Federal Data Leaks

Code42 IncydrTM Gov is the only FedRAMP Moderate Authorized Insider Risk Management solution for data exfiltration detection and response.

Overview

Federal agencies need to apply a Zero trust model to Data Protection to ensure all employees and contractors are not putting data at risk whether intentional or unintentional. Incydr Gov provides security teams visibility into all file movement to and from an endpoint, to quickly detect data leakage and data exfiltration activities. Code42’s Insider Risk Management (IRM) approach delivers on this promise with a foundation built on three core pillars:

⦁ Monitor all files, vectors & users

⦁ Meets NIST SP 800-53 moderate controls baseline

⦁ Non-disruptive to employee productivity or collaboration

Staying true to these three core pillars, agency security teams can shift their focus from maintaining technology like DLP to maturing the overall data risk posture. This fundamental shift in mindset results in delivering true security value by ensuring compliance, speeding time to value of security investments and building a more risk aware and collaborative culture.

The Problem

When an agency’s purpose is transformative, Insider Risk becomes the problem. As agencies transform their way of doing business and empower employees to be more collaborative, remote and cloud based, the risk of federal data being compromised (lost, leaked, stolen) via employee endpoints increases. We call this Insider Risk, and it accounts for more than two-thirds of data breaches and growing. Traditional data loss prevention (DLP) technology flies in the face of peoplefirst, innovative, collaborative companies. That’s why we’re pioneering a better way to protect federal data. One that fuels an agency's purpose and protects their mission critical data. It’s called Incydr Gov.

The federal employee and contractor's endpoints are the cracks in security’s armor today. Powered by the latest technologies, employees are downloading, uploading, emailing, Air dropping, messaging, posting, syncing, sharing, dragging and dropping corporate data 24/7—largely from their agency-issued laptop. The upside is that collaboration and sharing tools make them more productive. The downside is that these same tools make it easier to exfiltrate data and expose the agency to a data breach. Insider Risk is a direct result of employees having the access, means and motive to do what they want and/or need with agency data to get their jobs done. Every employee endpoint has become its own perimeter meaning security teams now have the daunting task to protect thousands of perimeters from data leaks.

The leader in Insider Risk detection and response WP2103251

Corporate Headquarters | 100 Washington Avenue South | Minneapolis, MN 55401 | 612.333.4242 | Code42.com

VnblX2

eOIEwX