code42

| | |
|---|---|
| Company name | Okta |
| Industry | Technology |
| Company size | 3,000+ |
| Use case | Data Leak |

okta

CASE STUDY

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

Fast-growing enterprise security company implements an Insider Risk Management approach to meet the data protection requirements of its innovative, global workforce.

Okta is the leading independent provider of identity and access management for the enterprise, with nearly 10,000 enterprise customers that include some of the most recognized and trusted brands in the world. Its vision is to accelerate a world where everyone can safely use any technology - and that includes its own workforce.

“We have a culture of growth, speed and transformation,” explains Matheo Lord-Martinez, IT Security Director at Okta. “Our [more than 3,000] employees are spread all over the world.”

## The Challenge

### Protect Business Data Across a Cloud-First, Global Workforce

Okta must be able to “deploy anything in the cloud and have our people use it,” says Lord-Martinez. But that’s not without its challenges. “We have valuable and sensitive data everywhere, and it’s very hard to protect that data, because it can exfiltrate in multiple ways,” explains Lord-Martinez. “And of course, the pandemic just accelerated all of this.” He and the rest of Okta’s security team aimed to solve this increasing data risk by prioritizing a data protection initiative that would bolster their control over cloud data. “The basic goal was to have full visibility of what’s out there from a file and data perspective,” explains Lord-Martinez.

## Purchase Triggers

- Improve control over employee file sharing via corporate cloud and email systems
- Ensure security team visibility into file usage and sharing during corporate migration from Microsoft365 to Google Suite

## Buying Requirements

The data protection initiative included a 129-point set of technology requirements which the security team created through collaborative conversations with stakeholders from across the business.

**Requirements included:**

- A cloud-based, cross-platform solution to support their mixed OS environment
- The ability to detect data exfiltration across a variety of vectors, with a specific focus on visibility into files shared from Okta's corporate cloud storage and email environments
- Trustworthy context into detected events to inform response
- No negative impact to employee devices and productivity
- Seamless integration with the Okta platform

## Evaluation Process

### Why Okta Chose an Insider Risk Management Approach over Policy-Based CASB

To solve their need, Okta considered a range of data security technologies, including traditional, policy-based tools like DLP and CASB. They measured each solution against their 129-point requirement list.

Code42 Incydr stood out for how quickly it could be implemented. It was the best option to solve their use case and see value within the month. Incydr's direct, API-to-API approach to integrating with cloud and email systems meant Okta would not need to set up and manage a proxy server in order to avoid accidental data leak via cloud file sharing and email.

When asked if this risk could be detected through built-in Google reporting, Lord-Martinez explained, "Incydr gave us a broader view of publicly exposed information. We could go into the admin console in Google Workspace and manually run a report of what has been shared externally, but that's it." Not only was this information available within Incydr, but Incydr was able to put it in context with the user's full file activity, regardless of whether it happened on the endpoint, in Google Drive or in Gmail. This provides Okta with a holistic understanding of Insider Risk requiring action.

> *"We have valuable and sensitive data everywhere, and it's very hard to protect that data, because it can exfiltrate in multiple ways. Incydr gave us a broader view of publicly exposed information."*
>
> Matheo Lord-Martinez,
> IT Security Director

## Benefits

### Exfiltration detection for all data types

As Lord-Martinez put it, "There's proprietary information everywhere, so it's hard to label when it comes to data. It's also very hard to protect all the data, because data can exfiltrate in multiple ways. I can exfiltrate in a Slack message or exfiltrate in an email or exfiltrate in a USB drive. It really doesn't matter what data it is, what matters is that it's being exfiltrated. I don't care if you're just taking a long text file or the whole source code — if there's something going on with our environment we need to expand the perimeter and protect our data.".

### Ability to avoid data leak through corporate email and cloud services

Okta's priority use case was the ability to protect data from being shared through corporate Google Drive, Gmail and Box instances. As Lord-Martinez puts it, not only were they able to do this for files shared by employees, but "we were able to find instances the other way around, in which people -- such as partners -- were sharing stuff with us. So we not only see what our people are sharing, but we can also see when we have documents shared with us that we shouldn't really have in our environment. Having that visibility is key. Incydr gives us the context and streamlined workflows to respond to what we see happening."

### Data security and visibility during a Microsoft to Google transition

Incydr played a key role in securing Okta's migration from Office 365 to Google Workspace in 2020.  It accomplished this through Incydr's direct integrations with Gmail, Google Drive, Microsoft Office 365 and OneDrive.

"We were able to make sure we had the capabilities to monitor data exfiltration, see publicly-shared things that shouldn't be shared — these are big concerns for every company," explains Lord-Martinez. As the move to Google progressed, Incydr helped Lord-Martinez and the security team monitor the movement of data, resolve when files were inadvertently exposed, and even see how successfully users were transitioning from Microsoft to Google to identify opportunities for user training.

### Seamless integration with the Okta platform

In addition to using Okta to perform user authentication and provisioning within Incydr, Okta's security team uses the integration to protect data used by their highest-risk users. "We assign risk to a user based on the type of data they have access to, and our high-risk user groups within Okta are automatically assigned to the high risk user lens within Incydr," says Lord-Martinez, "That helps us keep tabs on certain users, and helps us improve our security posture in general." And the integration between Incydr and Okta deepens the context needed to speed decision-making and response, providing the security team with user attribute information to speed investigations.

### A security agent that actually works on Mac devices

Like most innovative companies, Okta manages a mixed operating system environment. As Lord-Martinez explains, "Traditionally macOS is the forgotten software for enterprise, so any tool you find out there in the wild either doesn't work with Macs, or it works poorly, or it works with ten OSs before what we currently support. So it's nice that we've been able to use Incydr on multiple OS versions. We appreciate Code42 making a product that's equally as strong for Mac and Windows. I think you are one of the first security tools we have that supports M1 — everybody's slacking."

### A realistic approach to Insider Risk response

Incydr provides the security team with a unified view of a user's file activity whether that activity takes place on their endpoint or in corporate cloud and email systems. "In security, it's easy to get paranoid and think, 'Let's just block everything,'" explains Lord-Martinez.  But by prioritizing the activities that actually represent risk, Incydr allows Lord-Martinez and his team to enable users to work how they need to work, on any network, without disrupting legitimate work.

Lord-Martinez notes that Okta users are spread across global time zones, all with their unique work schedules. "But Incydr knows who people are, where they're located, and how they normally work, so I don't get false positives," he says. This accurate context allows the security team to take the best response to an action based on Okta's risk tolerance. "There's no one-size-fits-all playbook to respond to incidents that involve employee behavior," says Lord-Martinez.

> *❝ We assign risk to a user based on the type of data they have access to, and our high-risk user groups within Okta are automatically assigned to the high risk user lens within Incydr."*

## Outcomes

### Incydr improves Okta's risk posture through informed security decisions

Okta is using Incydr to make improvements to their Insider Risk posture. "Incydr is helping to drive policy decisions about our risk posture at a higher level," says Lord-Martinez. Okta leadership is now able to see the direct connection between effectively managing Insider Risk and enabling the speed, agility, collaboration and innovation that give the company competitive advantage. This has helped Lord-Martinez and his team to level-up the conversation on Insider Risk: "At a leadership level, we all care about Insider Risk," says Lord-Martinez. "Insider Risk now has visibility from the bottom to the top of the organization," says Lord-Martinez.

### You can't put a price on avoiding data leak

When it comes to how Incydr has helped Okta achieve its goal of protecting data from leak and loss, Lord-Martinez notes: "In security, benefits are really hard to measure — it's really hard to give value to all this data until it gets out. We're happy we don't have to find out. We're not living in 'disaster mode' because Incydr helps us mitigate our risk. We understand what the implications of data exfiltration are, and don't want to be a part of that. No negative impact is the best positive outcome."

## Recommendation to Peers

### Nothing to lose, lots to uncover

When asked what he'd say to others looking to better protect data from loss, leak and theft, Lord-Martinez states, "I'd say probably once you give Incydr a try you'll be like, 'Oh my god. What is going on?' because you didn't realize how much stuff is being exposed. Most of these tools just don't give you that ability. With Google Drive or Box, they just don't give you that ability natively, and if they do, it's not the way you wanted it to be from a security perspective. It's more from a management perspective. So give it a try. Ask for a demo. See if you can set up a test environment. Plug it into a couple of test cases and see if it works for you. I think you won't be disappointed."