CASE STUDY

mimecast

The 90s Called, They Want Their DLP Back

How Snowflake built a modern Insider Risk Management program

The Snowflake security team takes to heart that when it comes to data security, great success also means increased risk. In order to preserve the collaborative culture that made them such a stand-out organization while also keeping their critical IP safe, they needed to build an Insider Risk Management program that gave them visibility into data movement, without putting up productivity roadblocks.

Industry	Headquarters	Number of employees	Global reach
Technology	San Mateo, CA	2,000+	9 offices / employees in 19 countries

The Challenge

Full visibility without roadblocks

As a tech industry leader, Snowflake relies on their employees' ability to share and collaborate quickly in order to get their jobs done. So they knew right off the bat that productivity was something worth protecting. They also knew they needed to work quickly. "We had 90 to 120 days before going public to have a solution and a really tight story about our insider threat program," says Mario Duarte, Snowflake's VP of Security.

The Snowflake security team knew traditional data protection tools, like DLP and CASB, were too cumbersome and not effective at providing them the visibility they needed. "We didn't have a good story on the endpoint," says Mario. "I can see that you connected, I can see you downloaded something, but after that, I don't know what you did with it. It's like attempting to wrestle somebody with one hand tied behind your back."

Mario continues, "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."

The Search for a Solution

Mario and his team started testing DLP and CASB solutions to protect their data and gain visibility over their environment, but found them severely lacking. Not only were they clunky and complex, but one tool they tried even slowed down machines

> “If you’re trying to address growth and maintain collaboration, you can’t do it the old way. You can’t do it by blocking and encrypting - those days are gone.”
>
> **–Mario Duarte, VP of Security at Snowflake**

and actually interrupted their engineering workflow for a full 24-hours during a POC.

Mario elaborates, “the things that made us pause our deployments of traditional DLPs and CASBs is that they tend to approach things like ‘we are going to control data.’ To me, that approach was like, ‘the 90s called, they want their DLP back.’”

He continues, “those tools could tell us when something went wrong, but only if we asked them to look for it. We had no idea what risks were out there beyond what the DLPs and CASBs saw, and we knew it wasn’t everything.”

Most importantly, Mario realized that blocking would not be conducive to the collaborative culture that allowed Snowflake to grow and innovate so quickly. “We tried some of the more successful cloud CASBs and DLPs and, no matter which tool we tried, it always came down to them breaking productivity by blocking what employees were doing. [These tools] just can’t predict the type of work people do and whether or not that work is legitimate or risky,” he explains. “People are not machines. They get very creative to solve problems. To try to create rules that block a very individualized, unique problem--you know, people--it just doesn’t work.”

After ruling out rules-based data loss prevention, Mario looked for a solution that could provide full visibility to data risk instead. He started by asking his peers: “I belong to a forum of security leaders and I said ‘I hate DLP and CASBs are terrible; I want nothing to do with them, but I need to figure out how to protect our critical data.’ And it was like a Christmas tree lighting up with responses heavily recommending Incydr,” says Mario.

Achieving Visibility and Looking Ahead with Mimecast Incydr™

Enacting a right-sized response during employee departures

After bad experiences with a number of data loss prevention products on the market, Mario knew Incydr’s approach of detecting and responding to data risks without blocking would be a better fit for Snowflake’s data protection needs.

“You need to have visibility to understand what’s going on in your endpoint and your environment - and to be able to anticipate when something potentially is going to go awry, so you can takequick action,” Mario says. “With the advent of the cloud and employees working wherever, where you’re not really protected behind your onprem fortress, the new risks to data magnify the problem of endpoint security. So you can see how something like Incydr becomes a really important piece to signaling data risk coming in and going out of that endpoint.”

As they deployed Incydr and began integrating it with the rest of their security stack, Mario and his team saw value right away. He explains, “we have always prided ourselves on having pretty strong telemetry from our SaaS applications and in our own Snowflake services as well. With Incydr, we bring all that telemetry into the Data Cloud and

we contextualize it with other applications to get a much more complete collage of what's happening in the environment."

That integrated approach and the level of detail Incydr provides has allowed Mario's team to notice and address patterns that indicate potential insider incidents. For example, shortly after deploying Incydr, Mario's team found an employee had recently updated their LinkedIn profile and had also uploaded source code to their personal cloud storage - a common pattern that might indicate an exfiltration vulnerability. The team quickly responded by talking directly to the employee, determining the upload was unintentional and removing the code from the unsanctioned cloud storage. Mario says, "Without Incydr, we just wouldn't have known. We could have had some signals they were using iCloud, but not that complete picture. The ability to make those connections, it just wasn't there."

With Incydr, Mario and his team not only got a product that helped them effectively mitigate file exposure and exfiltration risks without disrupting legitimate collaboration, but also the support of the Incydr team, including members of the Security Success consulting team and a Technical Account Manager. "In order to meet our aggressive timelines, we needed to have a partner that could truly support our implementation and product use, and this is where the Incydr technical services team was instrumental. They work with so many different companies and, yes, we're all different, but there are some common threads, and the team can help you accelerate your program."

As Mario looks ahead to the future of his team and security at Snowflake, he views Incydr as a critical piece of their evolution. "Without hesitation, Incydr, and how it fits into our overall strategy, is central to our security program," he says. "Using Incydr, we see particular patterns and behaviors that suggest a potential insider moving data to untrusted systems. Anticipating rather than reacting - that's where we want to go with Incydr."

As for what he would say to someone facing the same challenges Snowflake was, Mario says, "When I talk to my peers there are a handful— maybe less than a handful—of vendor partners that I recommend. And Mimecast is one of those vendors because what they do and provide aligns with the collaboration culture that is being mandated by our senior executives and by the market. If you're trying to address growth and maintain collaboration, you can't do it the old way. You can't do it by blocking and encrypting - those days are gone."

About Mimecast

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscape, you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.