



Take the Blinders Off Remote Workforce's High-Value Data Movement

Innovation-powered tech company leverages Incydr to protect its IP while empowering user collaboration and ingenuity

Lyft, Inc. develops, markets, and operates a mobile app, offering vehicles for hire, motorized scooters, a bicycle-sharing system, and delivery service. Based in San Francisco, California, the company has more than 5,500 employees and operates in 644 cities in the United States and 12 cities in Canada. Lyft has quickly become one of the most recognized brands of our era, transforming fundamental aspects of our everyday lives and advancing the sharing (or gig) economy. One of the core accelerators of Lyft's growth and success is their company culture. "Lyft has always been a place of trust and cooperation," says Jae Ward, Security Analyst at Lyft. "We enable our users to work the way that suits them, and to use the tools and apps they need to get work done effectively. And with that comes a level of creativity that helps us be more innovative."

The Challenge

Data blind spots keep growing — especial ly in the cloud

Lyft deals with a wide range of valuable and sensitive data: "We have a lot of very sensitive IP — financial reports, source code and everything in between," says Ward, "And then we also handle a lot of very sensitive user data, too, when it comes to our drivers' license information and our riders' credit card information. "We want to make sure that stuff stays in our perimeter," says Ward, noting the potentially "catastrophic" impacts of leaking IP and other valuable company data.

Dealing with potential risk to this valuable and sensitive data ate up almost all of Jae's time, despite not being in her core job responsibilities. "We'd get paged in the middle of the night," when data exposure events were discovered — long after the fact — she explains. "We'd lose sleep at night — literally — because we just had no insight into what the heck was going on."

Of course, Lyft did have major investments in security tech in place, including the built-in security tools within their existing tech, including Google Workspace and other platforms that the company was using. But Jae and the security team still struggled to fully see all their critical data — and more importantly, to see it move. "Our data was this kind of ephemeral idea," explains Ward, "We knew it was there, we knew people were engaging with it and sharing it. But we couldn't really see how, and it was a huge blind spot in our company."

“The big thing we were trying to solve was that we had no idea where our data was going. We just had no visibility whatsoever. It was honestly just like running around with blinders on.”

—Jae Ward, Lyft Security Analyst

Cloud visibility was a particular blind spot. Case in point: Google Drive. “We use it for everything from disseminating training guides for our drivers, hiring materials, to internal things. If it needs to be shared, it’s in Google Drive,” explains Ward.

“So of course, we want to know what people are doing in Google Drive. For example, public sharing of our documents on Google Drive has been a problem for a long time,” says Ward. Yet despite Google Workspace tools, the security team had virtually no visibility into data movement on Google Drive. They didn’t even know how big their Google Drive footprint was.

As the company continued its rapid growth, it became increasingly clear that they needed to address these blind spots — particularly as they prepared for an IPO.

Purchase Triggers

- **Preparing for an IPO:** One factor driving the urgency was Lyft’s preparations for its IPO. “As our security posture evolved in the earlier days, data protection was less of a concern,” says Ward, “But as we worked toward our IPO, that was when people were like, ‘Okay, we should take this more seriously.’ And we very much did.”
- **Monitoring data movement:** “The big thing we were trying to solve was that we had no idea where our data was going,” explains Ward. “We just had no visibility whatsoever. It was honestly just like running around with blinders on.”
- **Monitoring cloud sharing activity:** Data activity on cloud platforms like Google Drive, DropBox, Box and OneDrive was a big blind

spot and focus of the initiative. “We just couldn’t tell if people were uploading things there. We could see things like people uploading things to our official Google cloud and our Amazon Web Service. But if they were sending it to a personal account or any other account, we just couldn’t tell,” says Ward.

Buying Requirements

The security team focused their search for a data protection solution on six essential criteria:

- **Platform-agnostic:** Lyft supports users on Mac, Windows and Linux.
- **Cloud-based:** A cloud-based solution was necessary to support Lyft’s decentralized workforce, including a large number of remote workers using corporate devices on private home networks.
- **Provide visibility to cloud collaboration apps:** Lyft needed visibility into apps including Google Drive, Dropbox, Box, OneDrive, and Slack.
- **Integrate with existing tech stack and home-grown automation:** The Lyft security team was already using Okta for identity and access management, as well as security automation technology Ward describes as “100% homebrewed in-house.”
- **Support compliance requirements:** Lyft needed a solution that enabled them to fully meet compliance requirements around data security and data privacy — including GDPR, CCPA, PCI and more — for its customer and driver data.

- **Foster collaborative, trusting culture:** The security team knew they needed a solution that enabled a trust-but-verify approach that aligned with the open, collaborative, trusting culture at Lyft — technology that was enabling rather than restricting and respected employee privacy.

Evaluation

Incydr proof-of-value makes immediate, compelling business case

As they considered various technologies, the Mimecast Incydr solution “definitely piqued my interest, to say the least,” says Ward. Their initial review confirmed that Incydr met all their core requirements, so they began a proof-of-value (POV) exercise to see if the solution delivered on all its promises. Immediately, Ward says the POV showed the Lyft security team that the data blind spots were even bigger than they’d realized. Ward recalls “finding public drives, much more data than we thought we had, and much more that was on public drives.”

The POV also demonstrated the easy extensibility of the Incydr solution through its pre-built integrations and API. “There are plenty of platforms out there that are effective, but they don’t integrate into ecosystems well,” says Ward. “Incydr and the various integrations — it’s seamless,” she says, “The API is very easy to work with — there’s not really restrictive or onerous rate limiting that you have to worry about — and it’s got integrations with pretty much everything: Workday, Okta, Google Drive, Gmail, Slack, you name it.”

Looking beyond current functionality, the Lyft security team was impressed by the roadmap for Incydr. “When I saw the direction Incydr was heading and understood the value in the additional support and services Incydr offers, I knew it would be a game changer,” says Ward.

“Incydr and the various integrations — it’s seamless. The API is very easy to work with — there’s not really restrictive or onerous rate limiting that you have to worry about.”

Benefits

Instant visibility to data activity in the cloud

“We went from not really understanding anything about what was going on with our data, to seeing everything,” says Ward. “We are able to see everything down to the minutiae of someone uploading a specific screenshot to Slack, up to the broader strokes of someone sharing an entire folder in Google Drive to an outside entity.” Incydr also provides the Lyft security team with critical, full visibility into their remote and flexible workforce.

“With Incydr, we have this assurance that, regardless of where our employees are working, we’re going to be able to see what data they’re accessing and where it goes,” explains Ward. “Incydr does a lot more than just tick boxes for us,” explains Ward. “It’s not just something that’s there that we have for auditing purposes. It’s something we engage with daily. We’re constantly monitoring it. We can rely on it. It’s kind of our source of truth, to put it really simply, more than anything else,” Ward concludes.

Using Incydr to machine the intuition of Lyft’s security team

Seeing everything was hugely important, but could have easily been overwhelming as well. Jae says that’s where Incydr’s risk prioritization methodology proved immediately impactful, enabling her to go from sifting through a litany of

alerts and false positives — to a high-fidelity risk signal that prioritizes risk based on their criteria and focuses her attention on what matters most. “It enabled us to very quickly and substantively tell Incydr: This is what we care about, and we want to know about it immediately,” explains Ward. The Lyft security team can focus in on things like source code and zip files, “So we know if we get a critical alert: It’s serious, and we need to action on it immediately,” she says. “It’s very much allowed us to focus in on what we care about and filter out the noise.”

Fitting seamlessly with existing workflows

Ward says the extensibility of Incydr again proved powerful when it came to acting on Incydr’s prioritized risk signal. “We have our home-grown Corp-Sec automation,” explains Ward, “and we very quickly were able to begin ingesting alerts from Incydr and filtering them down based on criticality and substance of the alert — and automatically generating tickets.” These tickets alert relevant individuals on multiple teams, including the security incident response team and Ward’s corporate security team.

This extensibility allows Lyft to maintain its investment in the security expertise they’ve already built and maintain existing security and incident response workflows — while vastly enhancing and accelerating them. “We get very actionable alerts that are substantive,” says Ward, “We know what is happening, we know what got

shared, why it got shared, and by who — and we can action it immediately. And Incydr enabled us to automate the process so there’s not just some poor person sitting there manually moving the alerts to the teams that need to know about them.”

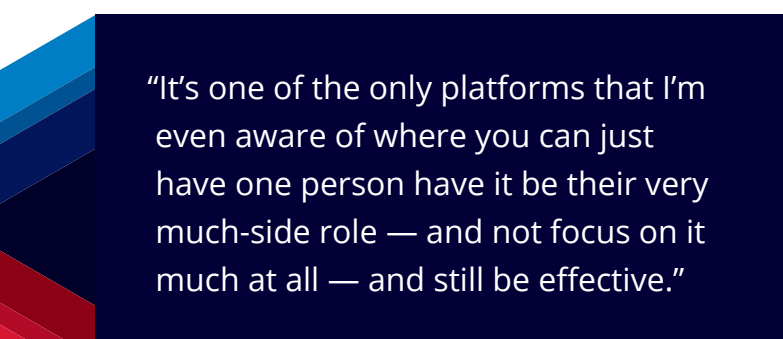
Context to drive right-sized response

Heavy-handed security responses just don’t fit Lyft’s open, trusting culture. “We very much try to be cooperative with our end users,” says Ward. Ward’s corporate security team and the Lyft incident response team leverage the broad, deep visibility provided by Incydr to quickly dig into alerts and determine a right-sized response based on the criticality of the situation. “For the high to medium alerts — unless they’re a high-risk or departing employee — we try to give them the benefit of the doubt,” explains Ward, “So, we reach out to say, ‘Hey, we saw this. It looks a little sketchy. What’s going on?’”

Higher criticality drives a more definitive response. “If somebody is exfiltrating source code, or we know someone is on their way out of the company, and they’re exfiltrating huge amounts of data, our Incident Response team will engage with our IT staff and they’ll do things like lock the device, lock out their Okta accounts — just to prevent them from exfiltrating any more data,” says Ward.

Rapid deployment & seamless integration into the lyft tech stack

Lyft rolled out Incydr in a matter of months and immediately began using many of the pre-built integrations, including Slack, Gmail and JIRA. They also integrated Incydr with their existing Okta identity and access management solution through the Incydr API, and they’re looking at using Incydr Flows with Workday soon. “It’s very much like plug and play in its truest form,” says Ward, “You configure what you want to see, and you can just



“It’s one of the only platforms that I’m even aware of where you can just have one person have it be their very much-side role — and not focus on it much at all — and still be effective.”

easily poke the Incydr API and say, ‘Hey, I want this specific data,’ and it brings it to you.”

“And it’s easy to read, too,” Ward adds, “It’s not in some archaic format or hard-to-read JSON. It’s: Here’s the date. Here’s the severity. Here’s what happened.” That intuitive output makes Incydr eminently usable for the security team: “You can ingest it, you can disseminate it, and do what you want with it — easily,” says Ward.



Outcomes

Much needed focus on lyft’s greatest data risks

The ability to fully see data activity — and more importantly, see what’s riskiest — is empowering not just for the Lyft security team, but to Lyft’s growth plans. Case in point: Incydr played a large role in Lyft’s preparations for its 2019 IPO. “We brought in Incydr just prior to us going public as a company, and it really saved our bacon,” explains Ward. “Going from complete blindness to seeing everything all at once was a little overwhelming,” she says, “But it gave us that assurance that we know what’s happening now.”

Full Visibility into Google Drive and Other Cloud Platforms

One of Lyft’s primary goals with Incydr was gaining visibility into data activity across Lyft’s vast cloud footprint, specifically targeting the widespread problem of public sharing of sensitive documents, something that was too difficult to accomplish natively in Google Workspace. “It’s largely just people being careless. It’s just people who are

Simple, scalable management

The Lyft corporate security team oversees more than 5,500 users. And while Lyft’s in-house automation team supports the automated incident response workflows, “When it comes to finetuning alerts, managing risk severity, exclusion lists, and any other issues, it’s pretty much just me managing Incydr,” says Ward, “And that’s okay! It’s one of the only platforms that I’m even aware of where you can just have one person have it be their very much-side role — and not focus on it much at all — and still be effective.”

trying to share something quickly — not thinking about how many other people can touch it with that public link,” says Ward. Incydr immediately proved much more useful than the built-in Google Workspace security tools that Lyft had previously used. “The Google tools don’t integrate well. They’re not the easiest thing to pull data out of,” explains Ward, Incydr integrated with Google Drive to give the security team visibility to the information they needed to know: “We were able to audit how many of those files existed, how many were overshared, and then disseminate that information to our IT team, so they can take action and just roll back those accidental shares,” says Ward.

Time - To - Response: From 24 Hours — to 1 Hour

The Lyft security team has a 24-hour SLA for responding to critical data security events. Before deploying Incydr, “We were about hitting that window — if not exceeding it due to the lack of visibility says Ward. “Now, the second we get an alert, there’s a whole bunch of events that kick off — and within one hour, we have someone eyeson investigating the problem,” explains Ward.

Insider Risk Management: From a Full - Time Job to 1 Hour a Day of Administration

Before deploying Incydr, Ward was spending the vast majority of her working hours juggling alerts and manually digging into potential issues. “I was dealing with these ‘what if’ scenarios almost daily,” she remembers. “Insider Risk is obviously a very serious problem, but it shouldn’t be something where a handful of people are manually handling it all, because it’s just not sustainable. And I think that was evidenced by how bogged down we were prior to implementing Incydr.”

Incydr transformed Ward’s work life: “When it comes to how much time we’ve saved, it really went from it being my primary function (despite it not being in my job description) to engaging with Incydr maybe for an hour a day — if even that.”

Smoothing Employee Departures & Other Workforce Pressures

The dynamic movement of workers between companies within the tech industry was amplified by the COVID-19 pandemic and the resulting “Great Resignation.” Lyft also made multiple acquisitions over the past few years. Ward and the Lyft security team are using Incydr to ensure that employees moving in and out of the company aren’t creating data security risks, such as exfiltrating or infiltrating IP to or from a competitor. “We’ve been very able to focus in on those specific groups and put them on the departing employee and high-risk employee lens,” says Ward, “Incydr enables us to say, ‘Okay, here’s the subset of users that we’re very concerned about — let’s watch them a little harder.’ It gives us alerts and rules that we can action on very quickly. It makes it so much simpler.”

Managing The Remote & Flexible Work Shift

“When COVID hit, everything changed — at both a personal and professional level — for everyone,” says Ward. As most security professionals experienced firsthand, the immediate shift to remote work “very much widens the scope of risk,” Ward explains, “Now you’re managing corporate devices on thousands of private networks.” With Incydr already deployed and integrated in their security workflows, the Lyft security team helped the company quickly adapt to the remote work shift — enabling remote workers while protecting business data. “We looked at this entirely new surface area and said, ‘How can we tune Incydr to keep track of these things?’” says Ward, “Because the problem doesn’t change — the surface area changes.”

Despite the magnitude of the shift, “Incydr gave us the toolset to be able to continue to approach data security in the same way, without having to completely revolutionize our entire footprint and how we approach data security issues,” says Ward.

Sanctioning Airdrop for Engineers turns Lyft’s Security Team into a Business Enabler

“Security can be a little adversarial in a lot of environments because that’s the nature of the beast,” says Ward. Incydr helped the Lyft security team further open up user policies and foster a culture of “yes,” giving them a “very easy, comfortable way for the trust-but-verify model,” she explains.

Case in point: AirDrop. “Before Incydr, we were like most other companies I know: No Airdrop. All bad. We don’t trust it. Bluetooth is scary. We can’t see what’s going in and out,” remembers Ward. “It shouldn’t be that way,” she says, “Just because a

tool exists and isn't manageable on the surface doesn't mean that you shouldn't use it. There are ways to fix these things. And with Incydr, we did exactly that." Leveraging Incydr's AirDrop monitoring capabilities, "We opened up AirDrop, and it was easy," says Ward. "We've had just two incidents where AirDrop was used in a suspicious way, and we were able to see it and act on it quickly."

Lyft's engineering team, in particular, continues to see tremendous business value through its use of AirDrop. "Our engineering staff was elated that they finally get to use AirDrop," says Ward. "They were quantifiably able to tell us that it increased their productivity and how much time they were saving — just not having to wait a few extra minutes to transfer files," she says.

Recommendation to Peers

Insider risk needs to be a bigger priority

Ward is a major proponent of the need for better Insider Risk visibility in the enterprise world. She warns that "scary hackers" perpetrating external attacks get the big headlines, "but most of the risk I've seen comes from internal actors." In addition to malicious and disgruntled employees, she says, "It's that a lot of people don't think about it when they touch this kind of sensitive data. It's easy to become complacent when interacting with sensitive data that could impact the business." Nevertheless, Ward says "I still see a lot of my peers not paying enough attention to what's going on inside their own doors — and with COVID and everyone working from home, it becomes an even broader issue."

Effective insider risk management needs to engage all stakeholders

A key to Lyft's speedy and successful deployment of Incydr, according to Ward, was the proactive planning and stakeholder engagement they did before Incydr went live. "It took some time. We engaged with a lot of different teams," she says. They worked closely with Lyft's legal and

"Insider Risk is definitely one of those things that a lot of people are sleeping on — and they really shouldn't."

compliance teams in order to deploy Incydr in a way that protected its users' privacy and met the requirements of GDPR, CCPA and other data security and privacy regulations. "We also reached out to security, IT staff, even just end users just to ask them, 'What are some things that you do on a daily basis that we might not be aware of?'" Ward says that this information-gathering gave them valuable insights as they determined how to use Incydr and how to prioritize data security risks. "Understanding what mattered to our company allowed us to work with our technical account manager [TAM] at Mimecast and say, 'Here's a list of needs. Here's our priorities. How do we make this happen?' And the TAMs and professional services team were able to just say, 'Cool, we'll get this configured for you,'" she explains.

It's time to take the blinders off

"Insider Risk is definitely one of those things that a lot of people are sleeping on — and they really

shouldn't," says Ward. For those who aren't sure another tool could solve the problem, or aren't sure they can make the business case for an Insider Risk technology, Ward has some concluding advice: "Just try a POV. Take the blinders off," she says. "In our case, the Incydr POV immediately showed us that our blind spots were bigger than we thought," Ward says, "The POV also made it really easy for us to make the business case for adding a focused Insider Risk tool like Incydr." Beyond the immediate visibility, she says the POV can show what a security team can accomplish with a more focused

signal of what's riskiest: "It not only helped us protect our IP, but it saved our security team a ton of time," say Ward. And perhaps most convincing, the POV will show how a purpose-built Insider Risk tool like Incydr can actually empower a more open culture — and better productivity and collaboration for Lyft employees. "It enables the trust-but-verify approach we needed," says Ward, "It's an easy win for us. It makes us look great, it helps them do their jobs better, and we don't lose anything in the process."



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.