

Lyft protects its IP while empowering user collaboration and ingenuity

Summary

Lyft needed to safeguard its intellectual property and other sensitive data, while maintaining a collaborative culture. By adopting Mimecast's Human Risk Management Platform, Lyft gained AI-powered, real-time visibility into data movement, allowing faster detection and response to insider threats without disrupting workflow. Contextual alerts reduced false positives and improved response times. This solution enabled Lyft to protect sensitive data, support remote work, and foster innovation, all while preserving employee trust and operational agility.

Key Takeaways

Challenges:

- Data visibility throughout hybrid and cloud environments, and across remote and on-site workers
- Security incident response SLA needed to be improved and time spent on insider risk management had to be decreased, while improving efficacy

Lyft chose to use the **AI-powered Human Risk Platform by Mimecast** to address its security needs, while supporting the collaborative and innovative culture.

Outcomes:

- Alert response time cut from approximately 24 hours to within one hour
- A measurable decrease in the number of unauthorized data access or leakage events after implementing enhanced security measures.
- Higher compliance rates with internal and external data protection standards
- Despite tighter security controls, Lyft was able to maintain or even improve employee productivity



About Lyft

Lyft, founded in 2012, is a global mobility platform connecting people through rideshare, taxis, car sharing, bikes, and scooters in nearly 1,000 cities across four continents. Millions of drivers have powered billions of rides, making transportation more accessible and connected for all.

The Mimecast logo is displayed in a dark blue, sans-serif font. It features the word 'mimecast' with a registered trademark symbol (®) to the upper right.

About Mimecast

Mimecast is a global cybersecurity provider, redefining how organizations secure human risk through precision-engineered AI, powered by AWS. Its AI-powered, API-enabled connected human risk platform protects organizations from the spectrum of cyber threats.

Benefits

Lyft rolled out Mimecast in a matter of months and immediately began using many of the pre-built integrations, including Slack, Gmail and JIRA. They also integrated with their existing Okta identity and access management solution through APIs, and they're looking at using pre-built workflows 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 easily poke the Mimecast API and say, 'Hey, I want this specific data,' and it brings it to you."

Lyft gained enhanced security, operational efficiency, and compliance by using Mimecast on AWS. The solution provided real-time monitoring and alerts, and generative AI within the solution enabled the team to quickly identify and address security threats. Lyft also benefited from streamlined auditing and reporting, which made compliance with industry regulations easier. Overall, these advantages reduced risk, saved time for security teams, and built greater trust with customers and partners.

Outcomes

With Mimecast, Lyft realized measurable improvements in both security and operational efficiency. The company reported a marked decrease in insider threats and a faster incident response time, reducing average remediation from days to just hours. Additionally, Lyft experienced greater visibility into data access patterns across its cloud environment, empowering proactive risk management. Ultimately, these outcomes allowed Lyft to safeguard sensitive customer information, reduce compliance costs, and support continued business growth with confidence- all while supporting the collaborative and trusting culture that drove Lyft's innovation.

Mimecast Powered by AWS

Mimecast's AI-powered integrated Human Risk Management Platform blocks advanced human threats that legacy security misses and reduces human risk across organizations. With complete deployment flexibility, and over 300+ integrations including those with security industry leaders such as CrowdStrike, Okta, Netskope, SentinelOne and Zscaler, Mimecast is trusted by over 42,000 customers.

Built on AWS, Mimecast uses native AWS services such as AWS Trainium, Amazon Sagemaker, and generative AI models via Amazon Bedrock to help deliver industry leading security.

Mimecast solutions are available on the AWS Marketplace and has the "Deployed on AWS" badge.

"Mimecast 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."

Jae Ward

Security Analyst

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

