mimecast

Protect sensitive data from potential exposure with Mimecast Incydr.

Preserve Data Safety in the GenAI Landscape

86%

of security leaders fear employees unknowingly leak data to GenAI tools.

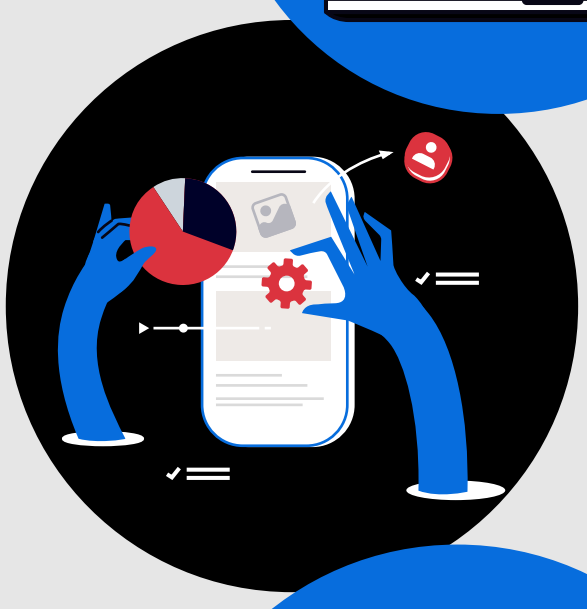
Data exfiltration is increasing due to Generative AI (GenAI).

Four essential rules to keep sensitive information secure

01

Get visibility into usage

It's important you understand the **GenAI tools employees are using as well as where those tools are accessed** across your organization. Visibility will be your foundation for finding unmanaged risk, shadow AI, and unsanctioned data movements.



02

Monitor data exfiltration in real time

Identify who is sharing data with GenAI tools. What data are they exposing? Where is it going? Continuous monitoring will help you **detect high-risk behaviors before any sensitive data has a chance to leave your organization.**

03

Investigate intent to reduce AI risk

Always work with stakeholders and leaders to **understand the why behind GenAI usage** among employees. It's critical to figure out the problems they are seeking to solve. With this context you can more easily separate productivity gains from genuine insider risk.

04

Enforce acceptable use policies with preventative controls

Build, define, and adapt an acceptable use policy for GenAI. Who can use it, what's allowed, and how can the results be leveraged? From there, **use technical controls to enforce it**, such as blocking high-risk tools and sites to protect high-value data sources.

mimecast

Ready to fully protect your data?

Securing your critical data means staying ahead of evolving threats. Talk to our team to see how Mimecast Incydr can help you protect sensitive data from potential exposure.

CONTACT SALES