DATASHEET

mimecast

Mimecast Incydr

Adaptive data protection for a changing world

The Problem

While external attacks are top-of-mind, the most frequent risks often begin inside your organization. Every day, employees share sensitive intellectual property like source code and customer data to shadow AI or untrusted destinations. This data leak and theft—whether intentional or accidental—jeopardizes customer trust, competitive advantage, and your brand reputation.

The Solution

See and stop data exfiltration from every modern work channel using one solution. Incydr intelligently adapts data protection as your organization's risk profile changes, ensuring the right employees have the right protection. Optimized for and by AI, with unmatched shadow AI visibility, AI-powered risk prioritization, and powerful agentic AI workflows.

Organizations choose Incydr because it offers unmatched visibility from day one, a wide range of adaptive controls to protect sensitive data and at-risk users, integrated agentic AI capabilities, and automatic prioritization of risk for better ROI and streamlined operations.

Despite 99% of companies having DLP solutions in place, **78% REPORTED DATA BREACHES.***

Every hour Incydr sees **OVER 6,000 DATA EXFILTRATION ATTEMPTS** to unsanctioned AI tools.**

* Source: Mimecast Data Exposure Report 2024
** Source: Anonymized Incydr Data, February 2026

Incydr Value

- **Get unmatched visibility on day one:** Detect theft of IP, source code, and PII out-of-the-box—no policy setup required. Incydr uses billions of signals to provide a behavioral baseline of all data movement across endpoint, cloud, browser, and email. CISO-friendly dashboards show common use cases like generative AI use, source code movement, cloud storage patterns, and more to understand your data security posture at-a-glance.
- **Adapt data protection as risk changes:** Deploy a range of adaptive controls that meet your organization's risk needs. Leverage everything from instant blocking to targeted education—powered by insights from your existing tools—to safeguard data without sacrificing productivity. Use watchlists to tailor controls for at-risk users.
- **Optimize your data protection program:** Incydr prioritizes risk that matters for better ROI automatically using AI and hundreds of built-in risk indicators. Automate triage and investigations with agentic AI, using Mimecast's dedicated Mihra agents or your own preferred LLM with MCP Server. Companies using Incydr reduce time to investigate high-risk incidents by 50%, and half of customers spend <4 hours a week on administration.

Incydr Use Cases

Use Case: Stop data from walking out the door
Departing employees pose a significant threat to a company's data security, with 80% of security leaders admitting that departing employees take valuable IP when they leave. This risk is heightened when employees transition to roles in competitive industries. Incydr automates departing employee monitoring by integrating directly with HR and ticketing tools. It identifies anomalous behaviors and allows you to quickly build a case from extensive activity history to share with an employee's manager or your HR and legal teams.

Use Case: Gain visibility and take control of Shadow AI & IT

Employees gravitate toward unsanctioned tools like shadow AI to work faster. Our own data shows thousands of data exfiltration attempts using unsanctioned AI every hour, with over half of attempts including source code. But traditional data protection tools are not built to detect and protect against this activity. Incydr allows you to gain visibility into all shadow IT activities including web uploads, pastes to GenAI, file attachments to personal email, transfers via Airdrops, and more. It provides a wide range of adaptive controls to educate, block, and contain these scenarios either organization-wide or targeted to specific users and data.

Feature	Details
SaaS Deployment & Extensive Ecosystem	• Cloud-native, SaaS architecture with a lightweight endpoint agent using 1% CPU and <50MB of memory combined with browser extension. • Cross-platform and environment agnostic – it works with what you've got: Windows, Mac, Linux, GSuite, or Microsoft 365. • Designed for the integrated and collaborative enterprise, allowing you to leverage pre-built integrations with SIEM, SOAR, XDR, IAM, HCM, and more. • Incydr Flows: Orchestrate controls to contain, resolve, and educate on detected activity using no-code automation with IAM, PAM, EDR/XDR, and other solutions.
Exfiltration Detection	• Incydr monitors endpoint, cloud, browser, and email from day one to see all untrusted file movement, without relying on policies or proxies. • Shadow AI and IT detection via monitoring of copy/paste and uploads to all untrusted websites and applications. • Dedicated connectors available for Microsoft 365 Email, Gmail, Box, OneDrive & Sharepoint, and Salesforce to maximize visibility and control. • Source code protection, including in-depth monitoring of Git commands and source code repositories.
AI-Based Risk Prioritization	• Automatically prioritizes events using AI and hundreds of customizable risk indicators based on three dimensions – files, users, and destinations. • CISO-friendly dashboards to view risk & exfiltration trends, adaptive control impacts, and track common use cases with easy user & file-level drilldown. • Access to exfiltrated files: Download and view the actual contents of exfiltrated files to verify their sensitivity and value. • AI-based Content Inspection available for PII, PCI, and custom data entities.
Wide Range of Adaptive Controls	• Real-time blocking: Block data originating from specific sources or going to specific destinations or allow users to request fully-auditable temporary exceptions. Prevent paste activity, removable media, file uploads, and use of desktop apps. • Integrated micro-trainings: Reduce everyday risky activity with video lessons that appear in real-time to correct employee mistakes as they happen. • Tailor controls: Apply controls to at-risk users using watchlists, prevent exfiltration of high-value data, or apply controls organization-wide. • Built-in case management: Quickly document and retain investigation evidence for high-impact incidents. Create reports for key stakeholders such as management, HR, and legal.
Native AI Integration for Unmatched ROI	• Deployed, fine-tuned, and fully integrated with other systems in weeks, with full monitoring and AI-based risk prioritization available from day one. • Bring your own AI LLM with MCP Server integration or leverage Mimecast's in-house Mihra AI agents to streamline investigations and automate remediation of alerts. • Payback in under 6 months, before most competitive DLP solutions are even rolled out with an average documented ROI of 172% over 3 years. • No regex policies to write or maintain.