DATASHEET

Mimecast Incydr

See and stop data loss caused by employees – without burdening security teams.

The Problem

While external attacks are top-of-mind for security professionals, the most frequent risks often begin inside your organization. Every day, employees misuse sensitive data by sharing valuable files with untrusted recipients and moving intellectual property to unsanctioned apps and personal accounts. This data leak and theft —whether intentional or accidental— jeopardizes customer trust, competitive advantage, and your brand reputation.

The Solution

Mimecast Incydr empowers organizations to protect sensitive data, such as customer lists, source code, and proprietary information, through advanced visibility and control over employee file activity. With Incydr, security teams can quickly identify, investigate, and respond to exfiltration events to protect data without unnecessary complexity. Organizations choose Incydr because it offers better detection and response than its competitors, all without creating extra work for security teams or slowing users down.

Insider threat events are increasing

32% YEAR OVER YEAR

and cost organizations an average $15M per incident.*

Insider threat is the

#1 HARDEST THREAT

to detect according to CISOs.**

* Code42 Data Exposure Report 2024

** Code42 Data Exposure Report 2024

Incydr Value

- **Eliminate blindspots.** Detect data theft of IP, source code and PII out-of-the-box on day 1 of deployment thanks to unmatched coverage that catches more than competitive policy-based solutions. Incydr has a payback period of under 6 months, and half of Incydr customers spend less than 4 hours a week on administration.
- **Automate effective response.** Manage insider risk by tailoring your response to the offender and the offense. Automatically correct mistakes, block unacceptable activity, and document and contain insider threats. Incydr helps companies reduce time to investigate and respond to high-risk incidents by 50%.
- **Never disrupt productivity.** Deploy to everyone – even power users – knowing Incydr doesn't slow devices down, block legitimate user activity, or bury security teams in extra work. In fact, it helps drive the behavior change needed to reduce risk to data so security teams have fewer alerts to address.

Incydr Use Cases

Use Case: Protect data when employees quit

Departing employees pose a significant threat to a company's data security, with studies indicating that 1 in 3 employees may take intellectual property (IP) with them when they leave. This risk is heightened by the fact that many employees transition to roles in competitive industries, potentially taking with them sensitive information such as customer lists, research data, and source code. The implications of this data loss can be severe-- impacting a company's bottom line

and competitive edge. Incydr automates departing employee monitoring by integrating directly with HR and ticketing tools. It speeds investigations using departing employee risk reports that include a lookback on historical activity, and allows you to quickly build a case from high-risk activity to share with an employee's manager or your HR and legal teams.

Use Case: Gain visibility and take control of unsanctioned apps and Shadow IT

Employees gravitate toward unsanctioned apps to work faster. In fact, 63% of employees use the tech they want to get their jobs done – including unapproved cloud apps. But traditional data protection tools are not built to detect and protect against this Shadow IT. 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, to get an understanding of your risk landscape. It provides a wide range of controls to prevent Shadow IT activity as well as drive behavior change across your employees.

Feature	Details
SaaS deployment & Robust Ecosystem	• Cloud-native, SaaS architecture. • Cross-platform and environment agonostic– it works with what you've got. Windows, Mac, Linux, GSuite or Microsoft 365. • Lightweight agent that does not impact endpoint performance thanks to agent specs of less than 1% CPU and under 50MB of memory. • Designed for the integrated and collaborative enterprise, allowing you to leverage pre-built integrations with SIEM, SOAR, XDR, IAM, HCM, and more.
Exfiltration Detection	• Incydr monitors endpoint, cloud, browser, and email to see when files are moved to places you don't trust, without relying on policies or proxies. • Source code protection, including monitoring of Git commands, as well as Shadow IT detection of GenAI, messaging apps, cloud sync, and more. • Actionable dashboards surface data exposure, training gaps, and corporate policy non-compliance. • Access to exfiltrated files. Download and view the actual contents of exfiltrated files to verify their sensitivity and value.
Risk Prioritization	• Uses its unique PRISM system to prioritize risk based on three dimensions – files, users, and destinations. • Has the ability to inspect data for custom and regulated data entities. • No regex policies to write or maintain.
Wide Range of Response Controls	• Integrated micro-trainings. Reduce everyday risky activity with video lessons to correct employee mistakes as they happen. • Real-time blocking. Prevent paste activity, removable media, file uploads, and use of desktop apps. • 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. • Incydr Flows. Orchestrate controls to contain, resolve and educate on detected activity using no-code automation with IAM, PAM, EDR/XDR and other solutions.
Unmatched ROI and Ease of Use	• Deployed, fine-tuned, and fully integrated with other systems in less than 2 months. • Payback in under 6 months, before most competitive DLP solutions are even rolled out. • 172% ROI over 3 years. • Low learning curve and a knowledgeable account team dedicated to your success.

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.