DATASHEET

Content Inspection for Mimecast Incydr

Protect sensitive data and support regulatory compliance without impacting endpoint performance

The Problem

Organizations need to protect their sensitive data from loss, leak, and theft. To accomplish this, security teams often utilize DLP technologies that inspect files for sensitive content patterns. These traditional content inspection methods frequently fail to deliver value due to productivity impact caused by analyzing files directly on endpoints. In addition, many organizations experience inaccurate detection because detection policies focus too narrowly on content patterns and don't offer context on other risks pertaining to the user, the file, and its movement.

The Solution

Incydr's AI-based content inspection capabilities avoid the downfalls of traditional content inspection techniques by executing analysis in the cloud using Natural Language Processing (NLP). This approach reduces work for security teams and ensures there is no performance impact on user devices. Administrators can set alerts for PII, PCI, and custom data entities to better detect, score, and respond to risk events involving PII, PCI, and other sensitive data types.

CISOs rank **Insider Risk** as the **most difficult threat to detect***

88% of security respondents find their **data protection solution is more work than anticipated****

Value

- **Strengthen compliance controls.** Protect files containing PII and PCI entities as well as other sensitive content types.
- **Accurately detect risk to data.** The Incydr PRISM system leverages three dimensions of context from users, data, and destinations to determine the severity of an event. By adding content inspection capabilities, Incydr enhances its ability to accurately detect file sensitivity.
- **Reduce impact to security teams and users.** Inspect files without endpoint performance impact that slows users down – all without complex Regex policies to write or maintain

* https://www.code42.com/resources/promo-resources/2023-data-exposure

** https://www.code42.com/content/2024-data-exposure/

Feature	Details
AI-based Content Inspection	• AI-based capabilities use Natural Language Processing (NLP) to inspect exfiltrated files and identify sensitive contents. • Out-of-the-box policies require minimal configuration while meeting industry standards for accuracy. • Cloud-side analysis avoids endpoint performance impact.
PII & PCI Entities	• Inspects file content for entities including but not limited to, US Social Security numbers, US Driver's License, US Passport, Credit Card, Email address, Banking details, and more.
Custom Data Entities	• Enables administrators to create their own custom Incydr Risk Indicators (IRIs) to alert on exfiltration events involving keywords and number strings unique to their corporate intellectual property. • This includes keywords such as "Attorney/Client Privilege," M&A code names or other secret project names, unreleased product names, and more.
Broad File Support	• Supports most exfiltrated file types, including images.
PRISM System Prioritization & Alerting	• Content inspection capabilities add another layer of context to the Incydr Proactive Risk Identification and Severity Model (PRISM) which is used to prioritize and alert on risk to data. • A file's sensitivity is determined using its source, classification labels, and other metadata. Now, file contents will also impact the sensitivity of a file. This strengthens Incydr's ability to detect, score, and respond to file exfiltration events. • Provides context on data sensitivity, adding to a library of 250+ Incydr Risk Indicators (IRIs).

Content Inspection Use Cases

Protect PII and PCI data

Protect personally identifiable information (PII) in a variety of scenarios, for example, during financial filings. Finance department employees compile sensitive information such as bank account numbers, IBANs, and SWIFT Codes in PDFs and spreadsheets to send to auditors as part of routine business activities. Incydr enables analysts to create specific rules to monitor financial-related PII, ensuring it is not exfiltrated through unsanctioned channels. These alerts help analysts quickly identify and address both accidental and malicious exfiltration of highly sensitive data, maintaining compliance with data-sharing policies.

Protect high-value company data

Protect proprietary information and intellectual property, such as prior to a new product launch. Incydr enables analysts to create custom file content IRIs tailored to detect specific product names and project details. By actively monitoring for potential leaks, Incydr ensures that any unauthorized exfiltration of information, such as to a competitor or to a social media site, is swiftly identified and addressed. This proactive approach allows companies to maintain the confidentiality of their upcoming releases, ensuring they protect their competitive edge.

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.