

Mimecast Sync & Recover

Automate data recovery for email with Mimecast's cloud-based solution, ensuring data protection and resilience.

The Problem

Email is a critical business communication tool and data repository, holding vast amounts of sensitive information. Protecting this data against loss or corruption is imperative yet challenging without the right tools. Organizations face difficulties managing spiraling inboxes and ensuring data resilience in the face of inadvertent or malicious deletions.

The Solution

Mimecast's Sync & Recover solution offers rapid and granular recovery of email data, including mailboxes, calendar items, tasks, notes, and contacts. As a fully integrated extension of the Mimecast Cloud Archive, it simplifies data recovery without the need for additional hardware or software. This solution is part of a layered defense strategy, combining with Mimecast Email Security and Continuity services to protect against malware attacks like ransomware, ensuring uninterrupted email access and data resilience.

The global average cost of data loss was around **\$142** per data record, totaling about **\$3.6 MILLION** per incident*

Data loss from data center outages costs U.S. businesses an average of **\$7,900** per minute**

Data breaches can lead to substantial financial losses, with compliance fines, penalties, and lawsuit settlements costing big brand companies between **\$1 MILLION** and **\$575 MILLION** since 2013***

Mimecast Value

- **Unified Management**
Simplifies the management of compliance archiving and data resiliency through a single platform.
- **Streamlined Recovery**
Facilitates easy configuration of recovery and search processes, reducing administrative complexity.
- **Multi-layered Defense**
Provides robust protection against data loss or damage due to ransomware and other malware.

* <https://storware.eu/blog/what-is-the-real-cost-of-data-loss/>

** <https://www.backupify.com/blog/the-real-costs-of-data-loss/>

*** <https://www.acronis.com/en-us/blog/posts/cost-of-data-loss/>

Feature	Details
Consistent End-User Access	Replicates Outlook mailbox folders to the Mimecast Cloud Archive, ensuring access from various devices even if primary systems are unavailable.
Cloud-Based Efficiency	Supports complex, global messaging environments like M365 and Exchange, with no hardware or software to manage.
Granular Retention Management	Allows administrators to manage policy-based retention of email content and metadata, with customizable rules based on email metadata and Active Directory attributes.

Sync & Recover Use Cases

Accidental Deletion Recovery

When merging email systems, it's ideal to be able to launch new domains as required without having to consolidate disparate email systems from day one. This ability allows businesses to implement new branding in email communications, while giving the IT team time to overhaul the underlying email infrastructure to accommodate the new business structure. With Mimecast, you can easily route emails to the recipient's correct mail environment. Active directory (AD) integration creates a smooth user migration process, ensuring message delivery and application access aren't disrupted.

Malicious Deletion or Corruption

The solution provides granular recovery options, allowing organizations to restore affected mailboxes, tasks, and contacts quickly, thereby maintaining business continuity and mitigating the impact of malicious activities.

Hardware Failure Recovery

Mimecast's cloud-based backup ensures that data can be restored to new hardware without the need for physical backups, facilitating a seamless transition and minimizing operational disruptions.

Compliance and Legal Discovery

The solution's granular retention management and search capabilities allow administrators to efficiently locate and retrieve necessary data, ensuring compliance with regulatory requirements and supporting legal processes.

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.

Aware Search & Discover

Aware's Search & Discover delivers AI-powered searches to quickly locate specific content and user activity with full context across Slack, Microsoft Teams, Zoom and other collaboration tools enabling rapid, secure investigations for Security, Legal, HR, or Compliance needs, all from a single platform.

The Problem

Today, IT and Security teams face increasing pressure to handle the growing volume of investigations tied to collaboration data from tools like Slack and Microsoft Teams. Additionally, the overwhelming volume of unstructured data leads to data sprawl, challenges in properly securing data in one, central location and costly requests from HR, Legal, Security, Compliance, and Privacy teams.

37% of messages containing PII and many being edited or deleted, adds to the complexity of complying with regulations like HIPAA, GDPR, DSAR and CCPA. Legacy tools fall short when dealing with the nuances of collaboration data, like emojis edits, deletions and unstructured formats, which makes it difficult to maintain proper audit trails, data archiving, access and disposal practices.

Without full visibility of the data and robust search capabilities to make the data accessible, these issues can escalate into costly, time-consuming investigations, exposing organizations to regulatory penalties and reputational damage.

IT and Security teams need a purpose-built solution offering centralized control, granular search, and contextual analysis to mitigate risks, maintain compliance, and streamline investigations.

The Solution

Search & Discovery, integrated into the Mimecast Human Risk Management platform, centralizes collaboration data providing real-time, AI-driven visibility. Purpose-built for compliance and security, it delivers full conversation context, preventing data sprawl, reducing costs, and ensures regulatory compliance through efficient, granular search capabilities.

- 1 in 53 messages are edited or deleted
- Personally identifiable information (PII) is present in 37% of all messages

Aware Search & Discover Value

- **Improved Human Risk Management.** Centralize governance for compliance, HR, and security investigations, addressing human risk swiftly and efficiently across your organization.
- **Complete Visibility.** Consolidate unstructured data from Slack, Teams, and Zoom into a single platform, providing real-time visibility and control for faster investigations and decision-making.
- **Full Context.** Access complete message threads, edits, deletions, and attachments to ensure defensible, accurate insights for comprehensive investigations across all collaboration platforms.
- **Federated Search.** Enable fast, federated searches and incident responses with immediate access to data across platforms, supporting customizable retention, privacy, and legal hold policies.
- **Efficient Compliance.** Ensure compliance with real-time AI-powered monitoring for reducing security risks, minimizing eDiscovery costs, and streamlining early case assessments and data exports for legal and compliance needs.

Product Overview

Feature	Details
Unified Platform and Workflow	One unified, immutable archive from across multiple collaboration platforms. Leverages native integrations that use APIs and webhooks to ingest, normalize and archive data. Integrate in minutes, not weeks or months.
Purpose-Built AI and NLP models	Aware enriches collaboration data using purpose-built models for identifying sentiment, toxic speech, inappropriate behavior, and more. Filter by negative, positive, or neutral sentiment. Identify inappropriate, offensive speech, or hate speech.
AI-Powered Search	Quickly find critical data across collaboration platforms with AI-powered, multi-faceted search. Use granular filters by keyword, user, or group, and wildcard searches to streamline investigations and improve speed and accuracy.
Examine Conversations in Context.	Instantly understand intent with full conversation context, including messages, edits, deletions, participant behaviors, and types of files included. Aware provides native collaboration format for accurate, contextual analysis and comprehensive search results.
Data Management	Organize, hold, or export data as needed for legal processes or audits. Remove data according to compliance regulations. Act on non-compliance with User Data Removal, Data Retention and Data Hold.
Data Access and Data Governance	Maintain precise control with granular security features. Limit access/visibility while Implement retention, privacy, and compliance policies across all data in real-time.
Platform Security	Enterprise grade security and infrastructure. SOC2 and ISO certified. Flexible Role-Based Access Control and SSO.
Simplified Investigative Workflow	Integrate seamlessly with existing security infrastructure using advanced APIs for event tracking, detailed reporting, and flexible, load-ready exports. Enable granular access controls, federated search, and automated actions like sensitive data removal and real-time alerts.

Search & Discover Use Cases

Simplified Data Compliance Management:

Streamline workflows by aggregating and organizing data to meet GDPR, FOIA, and CCPA requirements. Easily fulfill DSARs, identify Acceptable Use Policy violations, and export data to ensure compliance, prevent breaches, and avoid fines, legal penalties, and reputational damage.

Security, Legal and HR Investigations:

IT and Security teams can simplify investigations into Slack and Teams data with fast, accurate searches. Provide stakeholders with full context for rapid responses to data breaches, intellectual property theft, and inappropriate behavior, reducing investigation costs and minimizing operational disruptions.



Automatic classification rule setup – easily configurable for your organization's specific needs

Aware

Targeted Audience and Data Source

Target Classification Rules and Actions by ...

- Apply to one or many content integrations
- Specified source
- AAD Groups (Include/Exclude)
- Specified Individuals (Include/Exclude)
- People Sets -configurable list of individuals based on attributes (Include/Exclude)

Easy to Configure Classifications

Evaluate Files, Images (OCR) and messages

- AND/OR/NOT Boolean
- OOTB classifiers
- Configurable classifiers
- ML classifiers
- Collaboration specific classifiers

Proactively Automate Workflows

- Change/revoke sharing permissions
- Slack channel/user notifications
- Notify mailbox or user email
- Notify content author of violation
- Remove content for review in Aware
- API available

Aggregated Visibility & Risk Analytics

Understand the risk in your data and when certain policies are violated over time with Policy Reporting and Analytics



Integration and Analysis in Minutes



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 landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.

Aware Signal Datasheet

Most current version of the standard data sheet format and style

Aware Signal

Our AI-Powered Collaboration Security solution provides a secure and compliant digital workplace with always-on protection against sensitive data loss and non-compliance, addressing risks before they escalate, whether accidental, intentional, or policy-based.

The Problem

The explosive growth of digital communication on platforms like Slack and Teams has created a significant challenge for IT, Security, and Compliance teams. The lack of visibility and control over this unstructured data, especially in private channels and direct messages, leaves organizations vulnerable to sensitive data leaks and compliance violations.

Additionally, the sheer volume of unstructured data makes it increasingly difficult to maintain strong audit trails, data archiving, and proper disposal practices, potentially exposing companies to risks related to sensitive information such as insider trading, HIPAA violations, fraudulent billing, customer data leaks, and inappropriate workplace conduct.

Companies that ignore the escalating risk of unmanaged collaboration data face a difficult choice: accept the increased vulnerability to sensitive data leaks and compliance violations or rely on inadequate solutions like manual monitoring or legacy tools that lack the ability to understand the nuances of collaboration data (like emojis) and capabilities for custom detection and automated remediation. These approaches leave organizations exposed to costly fines, penalties for non-compliance, and significant reputational damage.

The Solution

Signal's turnkey integration centralizes collaboration data from Slack, Microsoft Teams, and other digital workplaces, providing near real-time visibility. With data secure and accessible, Signal's automated custom detection rules and remediation capabilities ensure always-on protection against sensitive data loss and non-compliance, addressing risks before they escalate, whether accidental, intentional, or policy-based.

17% of all messages contain 3 or more pieces of sensitive data

37% of all messages contain Personally Identifiable Information (PII)

Aware Signal Value

- Real-time, always-on visibility and control over collaboration data, all within a single platform.
- Purpose-built AI and NLP models deliver Accurate, real-time alerts, and automatic remediation of non-compliant behaviors and sensitive data leaks.
- Customizable detection rules for precise, custom detection rules for specific keywords to complex behavioral patterns.
- Configurable automated actions like auto-removal of sensitive information, real-time alerts to relevant personnel, or integration with your existing workflows.
- Simplified incident response with granular access controls, federated search capabilities, and seamless integration with existing security infrastructure.

Product Overview

Feature	Details
Unified Platform and Workflow	Leverages native integrations that use APIs and webhooks to ingest, normalize and analyze data from across multiple collaboration channels. Integrate in minutes, not weeks or months.
Purpose-Built AI and NLP models	Minimize false positives and quickly detect compliance violations, sensitive data leaks, and inappropriate content.
Customizable Detection Rules	Create precise, custom detection rules for company specific topics to complex behavioral patterns for toxic speech, inappropriate images, password sharing, and other regulations. Target or exclude specific sources within collaboration environments to increase the fidelity of signal to noise.
Full Contextual Event and Incident Details	Understand intent immediately with the surrounding context of flagged content. This includes surrounding messages, files, participants and modified versions of the conversation.
Automated Triggers and Remediation	Build automation to detect when policy violations occur. Configure specific actions like auto-removal of sensitive information, real-time alerts to relevant personnel, or integration with your existing workflows.
AI-Powered Policy Reporting & Analytics	Deliver aggregated visibility and risk analytics to help you understand data risks and policy violations over time.
Data Access and Data Governance	Maintain precise control with granular security features. Limit access/visibility while ensuring compliance with data governance and retention policies.
Workflow Integration	Integrate workflow into existing security infrastructure. Leverage advanced APIs for comprehensive event tracking and detailed reporting.

Signal Use Cases

Signal for Compliance

Signal provides IT, Compliance, and Privacy teams with complete visibility and control over collaboration data, ensuring regulatory compliance, mitigating the risk of costly fines, and fostering a secure digital workplace. Leveraging purpose-built AI and NLP models, Signal delivers real-time alerts and automates remediation of non-compliant behaviors.

Signal for Sensitive Data

Aware's Signal provides security teams with real-time, always-on visibility and control over their collaboration data. Custom detection rules instantly identify unauthorized sharing, triggering automated actions like notifications or auto-deletion. Leveraging purpose-built AI and NLP models, Signal minimizes false positives, ensuring the rapid identification of sensitive data leaks.



Automatic classification rule setup – easily configurable for your organization's specific needs



Targeted Audience and Data Source

Target Classification Rules and Actions by ...

- Apply to one or many content integrations
- Specified source
- AAD Groups (Include/Exclude)
- Specified Individuals (Include/Exclude)
- People Sets -configurable list of individuals based on attributes (Include/Exclude)

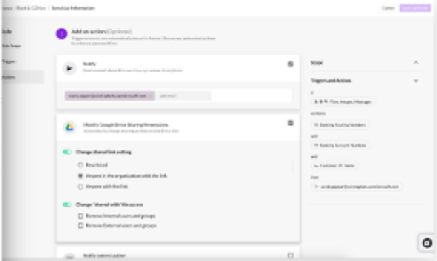
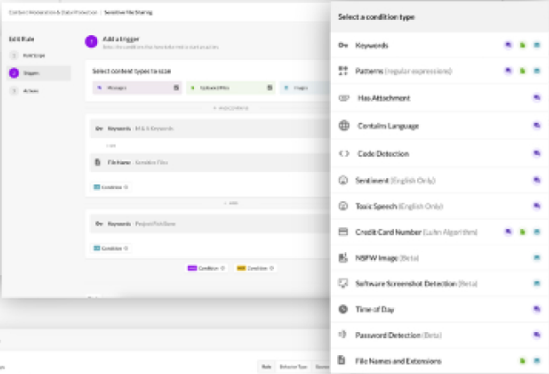
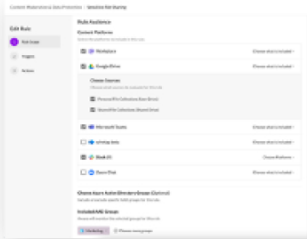
Easy to Configure Classifications

Evaluate Files, Images (OCR) and messages

- AND/OR/NOT Boolean
- OOTB classifiers
- Configurable classifiers
- ML classifiers
- Collaboration specific classifiers

Proactively Automate Workflows

- Change/revoke sharing permissions
- Slack channel/user notifications
- Notify mailbox or user email
- Notify content author of violation
- Remove content for review in Aware
- API available



Aggregated Visibility & Risk Analytics

Understand the risk in your data and when certain policies are violated over time with Policy Reporting and Analytics



Integration and Analysis in Minutes



Google Drive

Connect



Slack Enterprise Grid

Connect



Zoom Chat

Connect