

Mimecast Data Protection

Secure data from agents and the humans behind them

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASPO, E&I, and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Mimecast, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/MimecastResources



Join Events & Webinars:
carah.io/MimecastEvents



Discover Technology Solutions:
carah.io/solve



Learn About Procurement:
carah.io/MimecastContracts



Connect With Our Team:
Mimecast@carahsoft.com
(703) 230 7577

Mimecast Data Protection

Secure data from agents and the humans behind them.

8,000+

data exfiltration attempts to unsanctioned AI tools, every hour.*
Almost half of them include source code.* Your people moved work into AI faster than policy could follow.

THE PROBLEM

The workplace is changing faster than security can adapt, but the physics of data loss have not: data still leaves through a finite set of channels, endpoint, browser, cloud, email, and now the AI tools, agents, and connections wired into your systems. It is not a tooling gap for lack of trying: even with multiple DLP solutions, data exfiltration is still a major problem.

AI now moves data at machine speed through agents no policy anticipated. Mimecast Data Protection defends where the risk lives, the humans, the data in motion, and the AI acting for them, anchored on the constant: the data, the actor behind the movement, and the moment it attempts exfiltration. An agent pulling a large volume of records out of CRM looks identical whether the person behind it is a VP of Finance assembling a board pack or a sales director working out a notice period. Tools that govern the agent in isolation cannot tell those two apart, because the signal that separates them is human behavior, not agentic activity.

THE SOLUTION

Anchor on the constant, the data and the moment it leaves. Mimecast Data Protection sits at that moment of egress, sees every movement and whether a person or agent is behind it, and adds the context content-only DLP misses, who moved the data, from where, to where, and why, to answer the only question that matters: does this movement, by this actor, in this context, put the business at risk?

Mimecast gives teams one defensible view of human-agent risk across risk surfaces, improving operational efficiency when they do need to respond. And CISOs have one story to tell the board about how they are protecting humans, data, and AI.

Data Protection is available in two plans, Professional and Enterprise, shown on page 2.

AGENT RISK CENTER

EARLY ACCESS

Every other tool governs the agent. Mimecast governs the agent and the human behind it.

Agent Risk Center inventories every AI tool, agent, and MCP connection in your environment, classifies it as sanctioned or not, and ties each one to the person who deployed it. The action looks the same in all three cases below; the human behind it does not.

- **Accidental.** A well-meaning employee over-permissions an agent. It reaches data it never should. No malice, real exposure.
- **Compromised.** An agent is taken over by a threat actor and used to quietly reach high-value data.
- **Malicious.** A departing employee points an agent at sensitive data and exfiltrates at machine speed.

MIMECAST VALUE

01

See every risk surface instantly.

Mimecast tracks data movement, by humans and AI, across endpoint, browser, cloud, email, and agentic, with no policies to write or classification project first, for a complete human-agent exfiltration picture in weeks.

02

The same action can carry very different risk.

Every event resolves to the actor behind it and is scored on data, user, and destination, so adaptive controls match the action to the risk: routine work is coached and genuine threats are stopped.

03

A lean team can run the whole program.

Prioritized signals across risk surfaces, with agentic workflows doing the heavy lifting, turn hours of case-building into minutes.

USE CASES

Shadow AI and agents

For organizations whose people adopted AI tools and agents faster than governance could follow.

Uncover insider risk

For organizations securing data against departing, accidental, compromised, or malicious actors.

Protect source code

Secure your Git crown jewels, whatever your development lifecycle and tooling looks like.

Protect IP

Protect customer, employee, and other high-value data from reaching untrusted destinations.

* Anonymized Mimecast customer data, H1 2026.

Choose the plan that matches your program today

PROFESSIONAL

Insider risk protection across agents, endpoints, browser, and cloud.

Full detection, investigation, and response. For teams standing up or running an insider risk program.

ENTERPRISE

Everything in Professional, plus extended retention and deeper integration.

Longer event lookback, case archival, and full API access. For programs that need defensible history and want Incydr data inside their own stack.

CAPABILITY	PROFESSIONAL	ENTERPRISE
MONITORED SOURCES Where Mimecast watches for data movement		
Endpoints. File activity across managed Windows, Mac, and Linux devices		
Exfiltration detection. Detects files leaving trusted boundaries, no policies or proxies		
Exfiltration detectors for SaaS and cloud apps. Monitoring of cloud and SaaS destinations	1 INCLUDED	1 INCLUDED
Trusted activity. Filters out sanctioned, low-risk movement so alerts stay meaningful		
Metadata collection on exfiltrated files. File metadata captured at the point of egress		
Historical activity. Retained event lookback window for investigations	30 DAYS	90 DAYS
DETECTION, INVESTIGATION AND RESPONSE Included in both plans		
Risk Indicators. Hundreds of contextual signals that prioritize risk automatically		
Dashboards. CISO-ready view of exfiltration trends and control impact		
Watchlists. Tailor monitoring and controls to your highest-risk users		
Forensic search. Query file events across the whole environment		
Exact match file access. Pinpoint everyone who touched a specific file		
Cases. Package retained evidence for HR, legal, and management		
AGENT RISK CENTER Early access / govern AI and agent activity		
Agentic visibility. One inventory of every agent, AI tool, and MCP connection, classified		
AI Rulebook. Your AI acceptable use policy as an enforceable, living control		
Human-to-agent link. Each agent tied to the person who deployed it, across all risk surfaces		
INTEGRATIONS AND AUTOMATION Connect Mimecast to the stack you already run		
Pre-built integrations. Out-of-the-box connectors for SIEM, SOAR, XDR, IAM, and HCM		
CLI and SDK. Command-line automation and custom integration		
MCP Server and Mimecast AI agents. Automate investigations and triage with your own LLM or ours		
API. Programmatic access to Mimecast data protection data	BASE ACCESS	FULL ACCESS

Agent Risk Center is in Early Access and availability is subject to change at General Availability. Capability set accurate as of September 2026.

AVAILABLE ADD-ONS / ATTACH TO EITHER PLAN

CONTENT INSPECTION Inspect what is inside a file on the move for PII, PCI, and your own data entities.	INCYDR FLOWS Orchestrate containment across IAM, HCM, and EDR with no-code automation.	INSTRUCTOR Correct risky habits in the moment with short video lessons, as the mistake happens.	RETENTION PERIOD Retain data beyond the standard plan period, up to three years.	EXFILTRATION CLOUD CONNECTORS Extend visibility to more cloud services beyond the licensed connector.
---	---	--	---	--

mimecast

ABOUT MIMICAST

We secure humans, data & AI.

Your work moves through people, their AI agents and the data both touch, 8% of them generate 80% of your risk. Mimecast connects signals across the tools you already use, finds that 8%, and acts before a mistake becomes an incident. **Work Protected.**