Mimecast

Detection Strategy Guide

March 2026

Product Overview

Mimecast is a cybersecurity solution that helps organizations detect, analyze, and block advanced threats targeting people through email, including malicious attachments and URLs, and offers real-time threat prevention and forensic analysis.

Detection Strategy for Email Integrations

Detection

Expel integrates directly with email security providers and uses their data to quickly identify and investigate email and identity-based attacks to:

- generate Expel alerts for investigation
- provide enriched context to a threat
- offer decision support for incident scoping and severity identification

Expel consumes email security provider events through a mix of raw log analysis and security alert processing, which pass through our detection engine to identify signs of post-exploitation activity. When a threat is detected, our automated response bot takes action by enriching evidence fields with first- and third-party threat intelligence. Additional bot actions query a wide span of technologies in order to directly arm analysts with key pieces of investigative information and related events.

Email security providers do not provide full-body email text to Workbench analysts, but rather the alert data provided by the email security providers' devices. Full-text analysis of user-submitted emails is offered via Expel's Managed Phishing service offering. When events are promoted to Expel alerts, additional workflows are used to query to enrich the event with context.

Response

Email alerts are useful to identify and mitigate email threats such as phishing, business email compromise (BEC), and malware. Additionally, telemetry from other integrations with Expel is used to correlate activity across the kill chain to paint a more comprehensive picture of an attack beyond the email threat surface. For example, for an onboarded EDR or network security device, Expel can correlate the observation of a malicious attachment in the email security provider with the downloading and execution of that attachment in these integrations. If no other integrations are onboarded, analysts will use the context from the alert as well as Expel-internal enrichment sources (file/IP/URL lookups) to make the best determination of an alert.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for Mimecast

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Mimecast, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ Mimecast API 2.0
Supported event log sources	■ Attachment ■ Impersonation ■ URL (with a focus on click events)
Mimecast detection rules support	Yes.
Detection rules written by Expel	Yes.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events: ■ Query Mimecast URL Protection ■ Query Mimecast Attachment Protection ■ Query Mimecast Impersonation Protection ■ Query Mimecast Threat Activity
Hunting support	No. Hunting is not currently available for this integration.

Additional Details and Common Questions

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.

Use Cases Not Supported

Use Case	Reason
Abuse Mailbox (User Reported Emails) Support	Not included as part of the Mimecast MDR integration. Support for this feature requires the Expel Managed Phishing service.