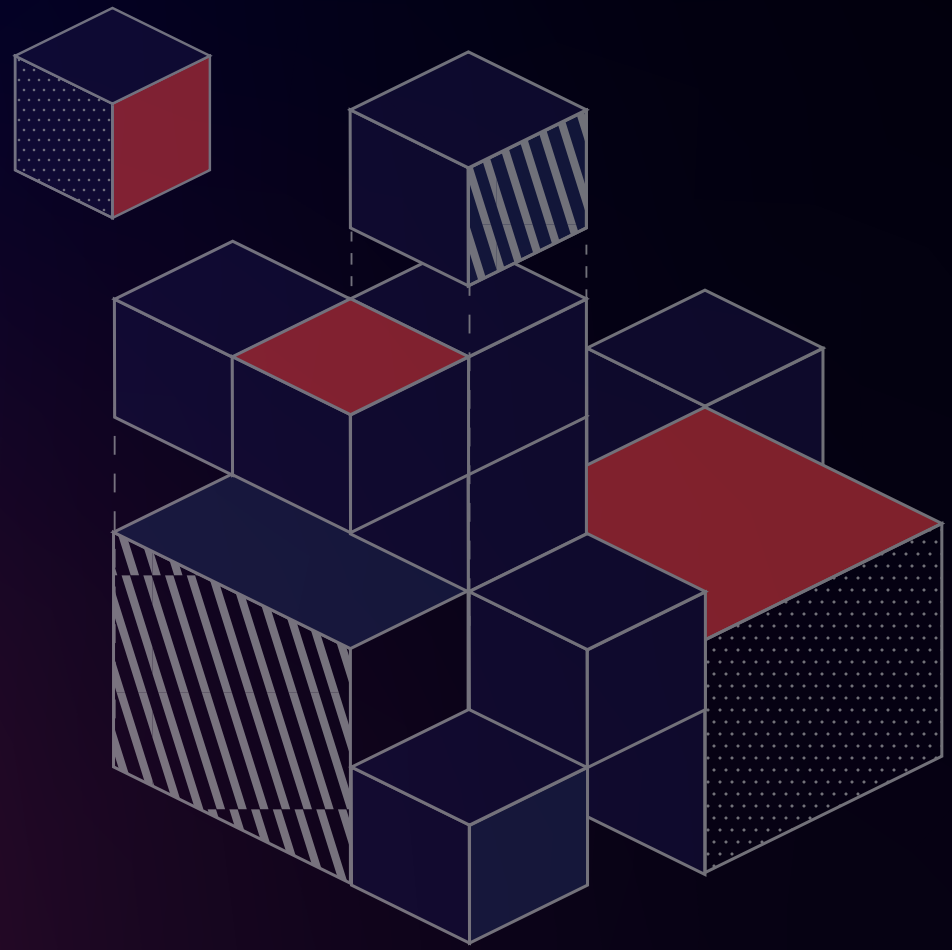
mimecast®

Integration Strategy Guide

Strengthening Your Security Program with Mimecast's Integrations and Open API



mimecast

Today's Security Challenges

Identifying cybersecurity risks and establishing more resilient defenses is essential to successfully operating and growing the modern business. Yet the path to protection is often bumpy. A dash to cloud and hybrid working models have significantly expanded the attack surface, adding more entry points for security teams to continuously monitor while threats slip through the gaps.

Over time, to keep pace with the demands of evolving IT and cybersecurity landscapes, organizations invested in an ever-increasing number of tools, which ultimately left them burdened with a collection of disjointed architectures and siloed components. This, in turn, resulted in complexity, technical debt, blind spots, and the inability of already over-worked SecOps teams to meet time-sensitive security events. To address burnout, the SecOps skills shortage, and security siloes, it's imperative to develop a streamlined methodology for strengthening cyber resilience, while reducing the manual task load. This security strategy overhaul is all the more urgent given the exponential growth of new multi-vector and multi-stage attacks – including phishing, business email compromise, insider threats, more sophisticated malware, cloned websites and account takeovers.

Reference Point: Enterprise organizations are using up to 45 security tools and a single incident requires coordination across around 19 security tools on average (IBM Study).

To combat the pervasive alert fatigue phenomenon brought on by the proliferation of disparate security tools, organizations are now focusing on quality over quantity, investing in automation, AI and actionable intelligence to help monitor, detect, and respond to threats efficiently and at scale. Whether your organization has a large Security Operations Center (SOC) or just a small team of IT generalists, requiring them to perform manual and repetitive tasks is a productivity killer—and an ineffective way to detect and prevent threats. Enabling automation is critical to solving this problem, but automation relies heavily on better integrations with the right security and IT management tools.

An open and pervasive API security strategy leveraged with a continuously growing list of off-the-shelf integrations will reduce the burden on IT and security teams, optimize security solutions ROI, and significantly enhance risk detection and response in today's dynamic threat environment.

This is exactly why Mimecast has continued to deliver a diverse set of data and programmatic services to our customers and technology partners. This strategy guide explores how increased automation via open API integrations can increase the efficacy of security solutions and improve the efficiency of security teams.

mimecast

Building your Security Ecosystem via APIs

A modernized security ecosystem must efficiently and effectively execute the “Protect, Detect, Respond” functions of the NIST Cybersecurity Framework (National Institute of Technology, CSF).

In the **Protect** phase, you need to take steps to quickly share data across your preventive controls. In the **Detect** phase, you need to collect data and intelligence to discover and investigate security anomalies that may signal an active security incident. Finally, in the **Respond** phase, you need automation to manage incidents and vulnerabilities, while minimizing the number of helpdesk tickets waiting in service queues.

mimecast

The Mimecast API

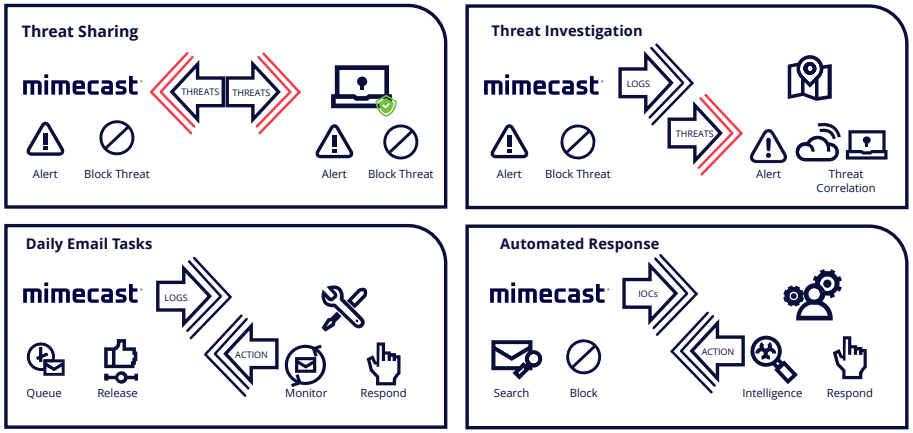
Complex security challenges have often led to the creation of complex security ecosystems. Mimecast is one of several security platforms that protect your organization, and we understand that to maximize overall effectiveness of all security services, Mimecast included, must be able to share threat data, automate regular or crucial tasks and help respond to threats across the organization.

Mimecast's range of complementary email and related security services are already tightly internally integrated as a result of the microservice-based development on the X1 platform.

These same microservices-powered APIs allow Mimecast to expose an extensive range of services and data sources with SIEMs, SOARs, perimeter protections, endpoints, ITSM solutions, threat intelligence platforms, and any other system that would benefit from an automated data exchange.

Bringing these capabilities into the systems you use every day will not only reduce the number of platforms you're having to retrieve data from, but it will strengthen your security ecosystem by delivering the information you need, where and when you need it.

Each category of Mimecast APIs below has a set of underlying services to help you with securing, automating, and better managing your IT and security ecosystem:



While the Mimecast API can and has been used to integrate into many types of third-party systems, this paper focuses on the four uses cases of integration that have shown to be most popular with more than ~5,000 of our customers—threat sharing, threat investigation, daily email tasks and automated tasks/response.

mimecast

Threat Investigation

Any organization that depends on a security incident and event management (SIEM) or extended detection and response (XDR) platform for its threat detection and security investigations, recognizes the fundamental need for the system to continually ingest key log and event data from the organization's primary security controls. Collecting and analyzing security data and investigating security incidents using both current and historical data is critical for efficient security operations.

Given that most security incidents include suspicious email or web activity, the timely integration of this log and event data must be part of any security integration strategy. The Mimecast API and its out-of-the-box integrations deliver multiple log types, such as URL Protect, Data Leak Prevention, Attachment Protect, Impersonation Protect logs, malware intelligence and more. This helps analysts and threat hunters focus on high-priority threats.

The retrieved data in conjunction with other security logs can detect compromised user credentials, command and control communications, data exfiltration, as well as the internal lateral movement of attacks. Furthermore, this data can be used to create visualizations and detections for the most attacked users in the organization, view blocked and visited web sites, and visualize malware rejection trends. When conducting investigations or threat hunting, the Mimecast SIEM/XDR integration enables analysts to search for malware by file hash, blocked URLs, blocked web requests, and sender IP and email addresses.

By delivering comprehensive visibility into the most prolific attack vector, Mimecast's integration into your preferred SIEM and XDR solution, such as CrowdStrike, Splunk and Rapid7, will significantly improve the performance of your threat detection, investigations, and response functions.

Mimecast also integrates into most Managed Detection and Response (MDR) and Managed Security Solution Providers (MSSP) to extending threat investigation capabilities to a third party.

mimecast

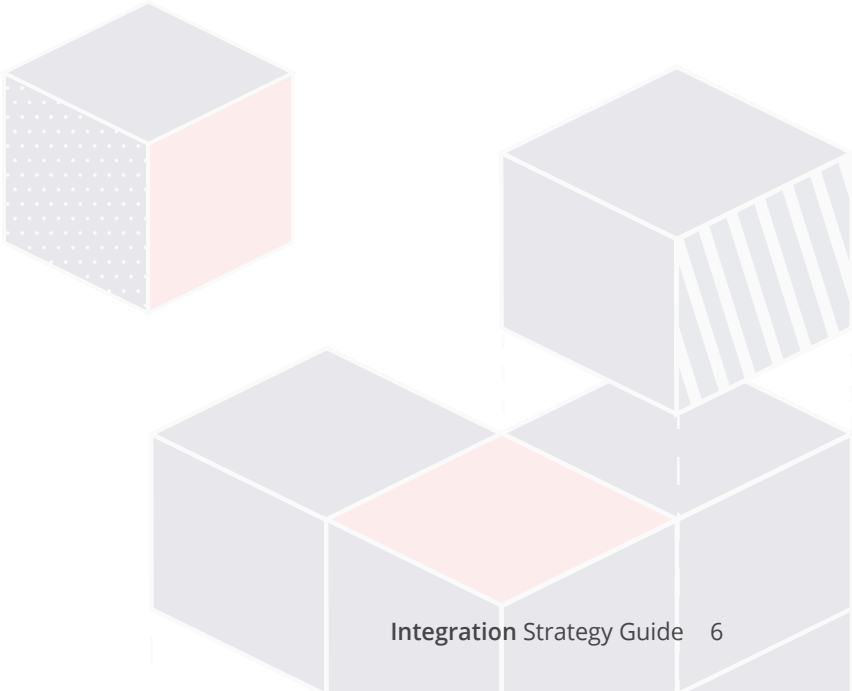
Threat Sharing

Threat Sharing is one of Mimecast's most popular customer use cases because it's integral to ensuring threat synchronization across key control systems, including endpoints, firewalls, and web security solutions.

For example, if the endpoint security system detects malware on a device, in addition to blocking its execution locally, it informs Mimecast by passing along a file hash to add to the Mimecast block list. This action will also trigger Mimecast to find and remove any previously delivered copy of the file, whether it is sitting in a mailbox or in the Mimecast Cloud Archive.

The reverse of this use case is also supported. When Mimecast detects and blocks a piece of malware, not only will it prevent the intended recipient from receiving it, but it also relays the information to an integrated security system. This enables the security system to update its block list in case the attacker attempts to deliver the malware via a less well protected channel like personal email or drive-by download.

Mimecast has built integrations with many of the leading security platforms, including CrowdStrike, Netskope and ThreatConnect. Two-way threat sharing accelerates and improves the defenses of organizations by pooling, automating, and applying threat intelligence where and when it is most needed.



mimecast

Automated Response

The integration of email security data into automation tools helps security teams work smarter, respond faster, and strengthen their cyber resilience against multi-vector threats. Security Orchestration, Automation and Response (SOAR) systems, Threat Intelligence and XDR platforms boost the efficiency of your team by automating threat analysis and incident response. Security staff can gather logs, block newly discovered malware or malicious IP addresses and even directly remove files in a matter of minutes. The ability to programmatically respond to threats relies on extensive data integrations that unify different cybersecurity tools.

Mimecast data can be both a source of information and a point of automation of security-related actions. For example, Mimecast URL logs can be used to add URLs to the block list for web security, while malicious or otherwise unwanted attachments detected by an endpoint can be automatically removed from emails.

Mimecast email security allows SOC teams to directly monitor and automatically remediate malicious emails that exist in users' inboxes or in the archive. The same malicious file hash detected can automatically be applied to endpoint, web, and firewall security tools. Remediated emails can be retained for compliance purposes, but tagged, so that they cannot be retrieved by users.

Mimecast has built integrations with many of the leading automation platforms, including Exabeam, Anomali and Palo Alto Networks Cortex XSOAR, to fortify defenses against the most advanced threats.

mimecast

Daily Email Tasks

Given limited IT resources and the unpredictability of IT demand, IT service management systems (ITSMs) are increasingly critical for the efficient management, prioritization, and scheduling of IT staff and resources. That's why many organizations have implemented specialized IT management systems, such as ServiceNow, Microsoft System Center Service Manager, SolarWinds Service Desk, among others, to efficiently manage their IT operations.

"One and done" whenever possible is the name of the game in the world of IT operations and ITSM. The need to forward open tickets from one IT function to another, especially for relatively trivial tasks, contributes to delays and negatively impacts user satisfaction. With integration, joint Mimecast/ITSM customers can conduct some of the most frequently performed Mimecast administrative functions directly from their ITSM console, avoiding context switching. If an IT analyst gets assigned one of these routine functions, they no longer need to reassign the ticket to a Mimecast administrator or get access to and learn the Mimecast administrative console; they can complete the task with just a few clicks from a single interface.

For example, a helpdesk analyst can search for/release/reject an email that is in an administrator hold queue, view/update managed URLs, create managed sender entries, view/update internal domains, decode Mimecast rewritten URLs, and view the status of Mimecast services all in the ITSM system. The integration between Mimecast and the ITSM does the rest. Highlighting the inherent bi-directional nature of the Mimecast APIs, these integrations improve the efficiency and speed of IT service delivery and remove some of the more mundane email management tasks from the organization's Mimecast administrators.

mimecast

Conclusion

As security controls evolve, it is imperative that the industry does not replicate the siloed, unintegrated product approach that has dragged down IT and security teams for years. The movement of IT and security services to the cloud provides a unique opportunity to rethink how security and related IT controls are implemented and how protections are automated.

While no one vendor will have all the necessary intellectual property to defend cyberspace, when multiple solutions are intelligently integrated, we at Mimecast think the good guys have more than a fighting chance.

Getting Started with Mimecast Integrations and Open API

Get started now by browsing through the dozens of existing integrations or requesting an application key to get started to build your own custom integrations.

Mimecast provides you with specific, documented, integrations that join the Mimecast APIs with those of many third parties. With these off-the-shelf integrations it is our experience that most can be up and running in under an hour!

Follow the steps and guidance here:

- API & Ecosystem - Enablement Hub
- Technology Partners
- Developer Portal

Access to the Mimecast API is tightly controlled and protected by security and compliance safeguards that protects the data in transit and from unauthorized access as well as denial of service attacks.