mimecast
SecOps
Virtual | 2021

API Strategy Guide

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

Today's Security Challenges

We face a new digital risk reality. The pandemic accelerated digital transformation projects for organizations around the world and also led cybercriminals to pivot their attacks. Meanwhile, IT and security teams have raced to prepare employees for new ways of secure working under intense time and budget pressures. This strategy guide will explore how increased automation via open API integrations can increase the efficacy of security solutions and improve the efficiency of security teams.

The rapid expansion of cloud services, notably Microsoft 365, which is in use by over a million organizations worldwide, and Google Workspace, which has 2 billion monthly active users, are fundamentally changing the way organizations are attacked. New multi-vector and multi-stage attacks – including phishing, business email compromise, insider threats, more sophisticated malware, cloned websites and account takeovers – are growing in parallel. Several significant cloud service outages in 2020, such as the Microsoft outage in September 2020, have also highlighted availability and compliance concerns and the gaps in organizational resilience resulting from over-reliance on a single cloud vendor.

Email continues to be the No. 1 source of cyberattacks and a significant point of risk for most organizations. Yet other collaboration tools (e.g. Slack, Microsoft Teams, and even Zoom) are also emerging as points of risk.

Whether your organization has a large Security Operations Center (SOC) or just a small team of IT generalists, no organization can waste their people's productivity on slow, repetitive, or manual tasks. But the need for greater automation to address these areas of wasted productivity leads directly to the need for more and better integrations with the relevant security and IT management tools, as visibility is a precursor to better prevention, detection, investigations, and response. And the move of security controls to the cloud does not change this. In addition, no application-centric platform, including Microsoft 365, can single-handedly provide the level of security or integrations necessary to keep up with the continuously evolving nature of cybercrime.

Given the increasing dependence on security related integrations, an open and pervasive API security strategy, leveraged with a continuously growing list of off-the-shelf integrations, is therefore required to reduce the burden on IT and security teams, get more value from security investments, and more adequately manage the risks inherent in the new enterprise IT landscape. This is exactly why Mimecast has continued to open up a diverse set of data and programmatic services to our customers and our technology alliance partners.

Building your Security Ecosystem via APIs

A strong security ecosystem is comprised of the ability to efficiently and effectively do the following when it comes to managing security threats: The 'Protect, Detect, Respond' portions of the NIST Cybersecurity Framework (National Institute of Technology, CSF).

To maximize the protections for your organization, you need to have systems and processes in place to protect it from threats, detect if your systems have been breached and to respond quickly. In protect, you need to take steps to quickly share data across your preventive controls.

In detect, you need to collect data and intelligence to help discover and investigate security anomalies that may be a signal of an active security incident. In the respond phase, you need automation to help address incidents and existing vulnerabilities to minimize the need for passing helpdesk tickets around and having them wait in service queues.

What is an API?

An Application Programming Interface (API) is a software service that enables separate applications or services to exchange data and service requests to each other. The applications can live anywhere on a network, whether on-premises or in the cloud, as long as they have connectivity and sufficient network bandwidth to support the necessary communications.

The Mimecast API

Complex security challenges have often led to the creation of complex security ecosystems to defend against them. Mimecast is one of several security platforms that protect your organization, and we understand that being an interconnected part of your particular security ecosystem is not a "nice to have." To maximize overall effectiveness, 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 on our platform are already tightly internally integrated as a result of the microservice-based development on the Mime|OS platform.

These same microservices-powered APIs allow Mimecast to expose an extensive range of services and data sources with SIEMs, SOARs, security 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 simplify the number of platforms you're having to retrieve data from, but it will help you to strengthen your security ecosystem by having 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, for purposes of explanation this paper focuses on the four areas of integration that have shown to be most popular with more than 1000 of our customers.

The remaining sections of this paper will focus on the need and some integration enabled use cases covering the automation of Mimecast services with Security Incident and Event Management systems (SIEMs), Security Orchestration Automation, and Response systems (SOARs), IT Service Management systems (ITSMs), and security endpoints.

Integrating with SIEMs

Any organization using a security incident and event management system (SIEM), such as Splunk, IBM QRadar, LogRhythm, Rapid7 InsightIDR, Microsoft Azure Sentinel or others, that depends on it for their threat detection and security investigations, understands the fundamental need to have key log and event data continually ingested into it from their primary security controls.

Whether the organization's security controls or the SIEM system itself is running on-premises or in the cloud does not change the fact that collecting and analyzing security data, and investigating security incidents using both current and historical data from these security systems 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 SIEM integration strategy. The Mimecast API and its out-of-the-box integrations deliver URL Protect, DLP, Attachment Protect, and Impersonation Protect logs.

In addition, Mimecast generated data such as service audit events and malware intelligence, as well statistics on general email traffic – messages delivered, rejections, queues, bounces, and held messages, are provided to integrations.

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

Clearly the integration of Mimecast to the SIEM of your choosing can help improve the performance of your threat detection, investigations, and response function.

Integrating with SOARs

Security Orchestration, Automation and Response (SOAR) systems, 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. However, a SOAR's ability to programmatically respond relies on extensive data integrations that unify different cybersecurity tools.

The flowchart style logic of SOAR platforms allows you to programmatically leverage Mimecast in an almost limitless number of scenarios and to use the Mimecast sourced data in many other platforms. Thankfully, using a SOAR also enables this with little or no scripting.

In particular, the integration of email security data into a SOAR system helps security teams to work smarter, respond faster and strengthen their cyber resilience against multi-vector threats. 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 to the block list at a firewall, or a malicious or otherwise unwanted attachment detected by an endpoint can be automatically removed from emails with Mimecast.

One common SOAR playbook example is automating the response to email account takeover, reducing the burden on IT admins and security analysts, and reducing the mean time to resolution.

The Mimecast service uses integration and email journal feeds from cloud-based email services like Microsoft 365 to allow 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 via email in Mimecast can automatically be applied to endpoint, web and firewall security tools using a SOAR. 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 SOAR platforms, including Splunk Phantom, Rapid7 InsightConnect and Palo Alto Networks Cortex XSOAR. Integrations such as these can be used to improve the effectiveness of your security response.

Integrating with ITSMs

IT service management systems (ITSMs) are increasingly critical for the efficient management, prioritization, and scheduling of IT staff and other resources. Efficiency is critical for the successful operation of an IT service desk, as resources are limited, and demand can be very unpredictable. This is why many organizations have implemented specialized IT management systems such as ServiceNow, Microsoft System Center Service Manager, SolarWinds Service Desk, and many others to 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, in particular 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 from within the ITSM console. 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 just do the task with just a few clicks from within the ITSM console.

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 current status of Mimecast services all by pushing buttons in the ITSM system. The integration between Mimecast and the ITSM does the rest. These types of integrations highlight the inherent bi-directional nature of the Mimecast APIs.

Clearly the integration of these Mimecast administrative services to an organization's ITSM can improve the efficiency and speed of IT service delivery as well as remove some of the more mundane email management tasks from the organization's Mimecast administrators.

Integrating with Endpoint Security Systems

Endpoint security systems, along with firewalls, user authentication systems, and email security, make up some of the oldest and most ubiquitous technical security controls deployed in organizations. Endpoint security systems act as the technology last line of defense against malware and other forms malicious activity that operates directly on a host.

A host or endpoint can be a laptop, desktop, mobile device, tablet, server, or virtual environment. While there are dozens of providers of endpoint security systems, such as CrowdStrike, Cylance, Carbon Black, Sophos, and many others, fundamentally they all focus on scanning files, executables, and the network traffic entering and exiting the host with the goal of detecting and blocking malicious files and activity.

Endpoint security systems provide security teams with the visibility they need to uncover security incidents that would otherwise remain invisible.

Mimecast's open API and off-the-shelf integrations enable the sharing of security intelligence with endpoint security controls. For example, if the endpoint security system detects malware on a device, in addition to blocking its execution locally it can inform 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 an Exchange 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 can also let an integrated endpoint security system know about it. This enables the endpoint security system to update its block list in case the attacker attempts to deliver the malware via a less well protected channel, such as via personal email or drive-by download.

Clearly, 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.

Conclusion

As security controls move to the cloud 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, once in technology generation opportunity to rethink how security and related IT controls are implemented and protections are automated.

While no one vendor will have all the necessary intellectual property to defend cyberspace, collectively when used together and 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.