Solution Brief

mimecast

Email Security 3.0

Ecosystem & Threat Intelligence

Resilience Extension

Make Your IT Team and Security System Smarter

Complex security challenges often lead to complex security ecosystems – a reality reflected by the fact that organizations are using numerous disparate technologies to address their security needs, with some employing as many as 75 different solutions. Making it all work together is about more than optimizing investments. It's about keeping your organization safe.

As the most widely-targeted attack vector, email is an incredibly rich source of telemetry and threat intelligence. Through a continuously growing library of APIs and robust threat intelligence, Mimecast makes it easy for you to leverage that data in ways that make both your IT team and overall security system smarter.

Email Security 3.0

Mimecast Email Security 3.0 helps you evolve from a perimeter-based security strategy to one that is comprehensive and pervasive, providing protection across three zones. These protections are enhanced by a wide range of complementary solutions, actionable threat intelligence, and a growing library of APIs.

Zone Defense	Extensions
Zone 1 At Your Perimeter	Continuity & Recovery
Zone 2 Inside Your Network & Organization	Web Threats & Shadow IT
Zone 3 Beyond Your Perimeter	Privacy & Encrpytion
	Governance & Compliance

Ecosystem & Threat Intelligence

Integration Options that are Fast, Easy, and Plentiful

Mimecast's library of APIs lets you quickly and easy plug into your larger security ecosystem, allowing you to:

- Take advantage of application data,
- Integrate with existing applications, and
- Optimize email and complementary security services.

Thanks to Mimecast's multi-tenant cloud infrastructure, integration options are extensive, and flexibility is the name of the game. And because our APIs run on the Mimecast private cloud, they offer the same security and compliance safeguards as any Mimecast service.

Real-World Scenario

A large restaurant chain was regularly targeted with phishing emails that required investigation and action by its IT team, a process that took from one to three hours for each email. Amount of time spent addressing this one problem alone? Roughly 6500 man-hours a year. There had to be a better way, and integration of its email security solution (Mimecast) with its SOAR provider (Demisto) turned out to be the answer. By integrating Mimecast's message search, URL decode, and block sender capabilities into Demisto, the company was able to reduce the time required to investigate and remediate phishing emails from 6500 hours a year to just 270.

The Mimecast API at Work

The Mimecast API library supports over 75 endpoints designed to support your existing business processes and applications. The following are just a few examples of how they can be used:

- **Configuration and administration,** to support configuration of various Mimecast components, such as users, domains, setup, and more, in the application of your choice.
- **Customer provisioning,** which allows Mimecast's registered Managed Service Providers (MSPs) and partners to automate customer account provisioning and streamline ongoing customer account management.
- **Security insights,** which supports enhanced logging, so you can programmatically download gateway and security log file data, track email messages, and interact with security policies.
- **Threat sharing,** which builds knowledge and amplifies the power of your security platforms.
- **Orchestration and remediation,** to support rapid remediation of threats.

- **Security investigation,** to support threat investigation and identification of issues in real-time through robust search capabilities.

Get Inside the Minds of Attackers

Mimecast's library of APIs is a conduit to sharing information from all our services to enhance your larger security ecosystem, and that includes Mimecast Threat Intelligence. Designed to give you both greater visibility and increased control, Mimecast Threat Intelligence provides information that is:

- **Contextual,** showing your organization's security performance and trends.
- **Actionable,** designed to help you take a more proactive approach to new and emerging threats.
- **Easily consumable,** to support communications with other stakeholders.
- **Instructive,** designed to help you better understand the threats your organization faces.

From malware detections and forensics to recently observed indicators of compromise and data about your most targeted end-users, Mimecast Threat Intelligence puts relevant, timely information at your fingertips. And with remediation capabilities accessible directly from the Mimecast Threat Dashboard, you can quickly respond to attacks, shutting them down and mitigating damage.

Stronger together

Make your entire security ecosystem smarter with API and threat intelligence capabilities that allow you to:

- Choose from over 75 end-point connections
- Search and surface Mimecast Archive data from just about any application
- Automate provisioning and streamline ongoing customer account management
- Build new services quickly and securely with an open standard REST API
- Get a deeper understanding of what threats have been blocked and why
- Make better informed decisions about staffing and security technology investments
- Leverage existing security investments more strategically