# Top Proofpoint Benefits vs. Mimecast

| Feature | Mimecast Method | Proofpoint Method | Technical Value Prop | Executive Value Prop |
|---|---|---|---|---|
| **Sandbox Analysis** | • Can't analyze URLs in attachments<br>• Can't analyze files at URL destinations (dropbox, etc.)<br>• Can't analyze password protected attachments<br>• Missed **43.5%** of known exploits upon initial infection<br>• Only **25%** effective at identifying threats in under 5 minutes<br>• Average sandboxing time of 10 – 15 minutes per attachment<br>  • (Data from independent NSS labs test of Mimecast) | • Analyzes URLs in attachments<br>• Analyzes files at URL destinations<br>• Analyzes password-protected attachments<br>• Identifies approximately **80%** of threats in under 5 minutes<br>• Average sandboxing time 2-3 minutes | Proofpoints sandboxing is **5x** as fast on average, and over **3x** more effective identifying threats in under 5 minutes. | **90%** of threats come in over email, but most orgs invest an average of **8%** of IT spend in email protection. Proofpoint helps protect users where they work and where the problem is: Email. |
| **Impostor / Impersonation Email** | Mimecast relies on the customer to set the parameters for when they block impersonation email, and then uses static analysis of the traffic. Mimecast also primarily focuses on executives, even though attackers focus on any employee with access to data. This can lead to false positives and human error– specifically around Internal User Names and Reply-To Address Mismatch conditions. | Proofpoint uses dynamic analysis of your traffic, header information and message content to allow for detection of malicious anomalies via pattern recognition. | By focusing on the entire organization, and by detecting **1,000+ email fraud scheme types**, we help prevent blind spots and uneven protection, which allows us to block impersonation attacks whomever they target. **In Q2 2017 alone, we caught 35,000 specific impostor attacks.** | Business Email Compromise (Executive Spoofing) cost American businesses a total of **$5.3 billion** as of 2015,with over **40,203** organizations targeted, according to the FBI. |
| **Spam / AV Filtering** | Mimecast relies on grey-listing for front-end spam filtering. This can lead to delays in mail or even loss of mail from new senders and customers.<br><br>In addition, while Mimecast has multiple quarantine folders, Mimecast quarantines all spam messages in one spam folder. This can potentially allow end user access to malicious messages. | Proofpoint relies on machine learning technology and a shared intelligence platform to actively analyze incoming messages and protect your org.<br><br>We also provide multiple spam classifications for quarantine. This allows you to provide end user access to messages without sacrificing the organization's security. | Our advanced visibility and filtering methods provide both a **99% spam filtering SLA and a 100% Virus SLA, with less than 1 minute email latency.** | Proofpoint topped the Gartner Market Guide for Secure Email Gateways as the **"sharpest focus on email security issues".** |
| **Post-Delivery** | To identify a malicious message that was previously delivered and notify an organization, Mimecast requires the end user to forward the message to an internal or external recipient. | Proofpoint has visibility and click-data for delivered messages, which allows us to identify malicious messages that made it through the solution and integrate with exchange and remove those messages from the end user's inbox, even at rest. | **99%** of advanced attacks require the end user to interact with the message to run malicious code. Increased visibility and message tracking means IT teams can attend to issues quickly and effectively. | Malware breaches remain undiscovered for an average of **146 days,** called the Breach Detection Gap (infocyte.com). Proofpoint's focus on post-delivery intelligence will help you prevent those issues. |
| **Forensics & Data Access** | Mimecast provides very limited data about advanced threats that are blocked, and no data about threats that get through their service. Customers have no actionable data or forensics to aid with remediation and comprehension.\<br><br>According to their website, Mimecast filters approximately **307 Million emails a day.** | Proofpoint provides in-depth forensic data from our sandbox events, enriched by our shared intelligence network, and curated by our team of over 100 dedicated global threat researchers so that you can quickly and efficiently react to attacks against your organization if necessary.<br><br>Proofpoint filters over **1.5 Billion emails a day**. | Proofpoint provides over **60** customizable, real-time reports, in addition to sandboxing data. **With Proofpoint, you will know the who, what, where, when and why of every attack.** | Proofpoint protects **53%+ of the Fortune 100**. We have over **6000+ enterprise customers** and **protect over 100M enterprise mailboxes**. With Proofpoint, your organization has access to |


© 2016 Proofpoint, Inc.

# Top Proofpoint Benefits vs. Mimecast

| Feature | Mimecast Method | Proofpoint Method | Technical Value Prop | Business Value prop |
|---|---|---|---|---|
| **Integrated Platform** | Mimecast licenses siloed, 3rd party products to operate their solution, and these 3rd party companies don't share threat intelligence. This means Mimecast is ineffective against cross-vector attacks. They can't protect against today's truly advanced threats. | Proofpoint can protect your organization across SaaS, Social Media, Mobile Devices, Incident Response, Domain Authentication, amongst others, and we share information across these solutions to create a truly integrated platform. We see 1.5 billion daily emails, 20 million mobile apps, 200 million social media accounts, and 250,000 malware samples, daily. | **Social Media Attacks have increased 150% YoY, and often employ lures into email and mobile device compromises**. Having our integrated platform can prevent such attacks. | Bad actors are attacking you and your customers in everyway you communicate with them. Proofpoint factors this in, and protects your people wherever, and however they work. |
| **Ecosystem Integrations & Extensibility** | Mimecast has limited integrations with vendors. This creates a lot of work and chance for error as admins work to make use of the data provided. | Proofpoint integrates with 50+ vendors with industry leading Firewalls, SIEMs, IDS', SaaS deployments, and more to share intelligence and proactively block across your entire ecosystem. We do this though our Incident response tool called Threat Response, our threat and configuration APIs, and our Technological Add-ons for Splunk. | Proofpoint's integrated ecosystem solutions can help you decrease investigation time by more than **50%**, and facilitate threat containment operations **20x** faster than average. | By speeding up identification and response to threats, your IT team will be able to reduce the chance of issues spreading and compromising the entire organization. |
| **Support** | Mimecast charges a premium for limited support. Reviews from Mimecast customers say that there is no support for installation and configuration of the solutions and settings. This leads to reduced effectiveness from Mimecast's published ratings. | Proofpoint includes a full installation and customization of our solution, in addition to 24/7/365 support after implementation with every purchase. | Proofpoint Professional Services will import safe / block lists, configure rules and settings, and make sure you hit the ground running on day one with a fully functional deployment. | Proofpoint has a five nines up-time SLA **(99.999%)**,<br>**90%** of cases are solved with L1 support with an average time to answer of **24s,** and **90%+** YoY customer renewal & satisfaction rating. |
| **Adaptability** | Mimecast licenses its filtering technology from 3rd party companies. The various 3rd party companies don't share information. This makes adapting to zero-day threats difficult, and leads to reduced efficacy. | Proofpoint owns all its own technology, which seamlessly shares intelligence and integrates. This allows us to quickly adapt to new threats, actors, and attack vectors. | From 2016-2017, ransomware increased by **33%**, Email Fraud losses increased by **3,100%**, and Malware variants increased by **XXXX%** | Attackers treat compromising your organization like a business venture, and are always trying to stay ahead of the curve. Proofpoint adapts quickly so you remain a step ahead as well. |
| **Archive** | • Mimecast's 7 second search SLA only pertains to end users archives<br>• Mimecast can only support 58 file types, and as for IM programs, they can only sync Skype / Lync for business<br>• Mimecast charges extra for features included in the Proofpoint archive at no extra charge. Power tools (replicates folder structure) and Archive Sync and Recover (exports data to .pst format).<br>• Mimecast archive doesn't qualify for FINRA and SEC regulations<br>• Limit of 5 e-discovery cases running simultaneously. | • Proofpoint has a 20 second SLA for searching the archive across the board, whether it be an end user searching their personal archive, or an admin searching terabytes of archived data.<br>• Proofpoint can archive 500+ file types, including multiple business and personal IM programs.<br>• Proofpoint offers a fully-functional archive solution without having to purchase additional add-ons.<br>• Proofpoint archive qualifies for FINRA and SEC regulations, amongst others<br>• Proofpoint does not limit the amount of e-discovery cases the admin can run simultaneously. | Proofpoint's archive can store **9x** more file types / data sources than Mimecast, with no limit in accessibility to your archive, all the while qualifying for stringent supervision requirements. | Proofpoint's Archive compiles and protects your data with unmatched efficacy, while providing your admins and employees uninhibited access at a moments notice. |


© 2016 Proofpoint, Inc.