**Mimecast Features Breakdown**

By Charlie Altenbach

**Core Functionality**

* + **Spam Filtering**
    - Spam Filtering is part of the core Mimecast Package.
    - Mimecast’s Description: With Mimecast’s email spam filter, you can:
      * Block spam – Mimecast’s email spam filter SLA stops 99% of spam with 0.0001% false positives.
      * Minimize disruption with an email spam filter and security solution that also protects against attacks.
      * Enhance productivity by enabling users to manage their own lists of blocked and permitted senders, reducing calls to the help desk.
      * Support mail validation technology including DKIM and DMARC.
    - We have found the SPAM filtering to work very well.
  + **Additional Content Filtering (Objectionable material, customized rules, etc.)**
    - Mimecast has multiple options when scanning attachments.
      * Block by File Type
      * Scan for Pornographic Images
      * Scan for Encrypted Archives
      * Scan for Unreadable Archives
      * Scan for encrypted Documents.
  + **File Attachment Screening (Traditional Signature Based AV)**
    - Mimecast has multiple layers of detection when scanning attachments.
    - **Mimecast’s Description:**
      * Stop malware and viruses – Secure Email Gateway provides 100% anti-malware protection including zero-hour protection and 100% availability SLA.
  + **Spoofing Protection**
    - You can set up address-based Anti-Spoofing policies
  + **Impersonation Protection (SPF/DKIM/etc.)**
    - Impersonation Protect is an add-on module at additional cost (included with other Target Threat Protection Tools (i.e. bundled with attachment and url protection)
    - Mimecast’s Description: Impersonation Protect is an advanced email security technology that protects employees against targeted social engineering attacks in email, often called whaling or CEO Fraud. Extending our existing Secure Email Gateway anti-spam and anti-virus services:
      * + Real-time protection against malware-less social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud.
        + Backed by comprehensive protection from Mimecast’s threat intelligence infrastructure and Messaging Security teams.
        + Protects against unknown or newly observed domain names used as part of the attack.
        + Protects against display name or friendly name spoofing.
        + Protects against domain similarity attacks.
        + Ensures end users are protected at all times by visibly marking suspicious emails.
        + Rapid deployment for instant protection with no client software needed.
* This has been an interesting module to administer. It has taken a bit more management in that we have had to implement a Bypass Policy. (Many of the Mimecast policies, including this one include a built-in Bypass Policy shell.) Even with the maintenance, it has proven to be worth-while.
* Based on the “Number of Hits” set by the admin, it will trigger the policy. This policy can look at the following criteria:
  + - * + Is the sending domain similar to the internal domain?

You can set level of similarity.

* + - * + Is it a newly observed domain?
        + Does the sender have the same prefix as an internal user”

i.e. jim@internaldomain.net vs. jim@gmail.com

This is the item that is causing us to use a bypass.

* + - * + Does the sender match the reply-to?
        + Is it a threat known to Mimecast?
    - Phishing Defense
      * Included in Impersonation Protect
    - Email Server to Email Server Security (TLS Support)
      * Mimecast has the ability to either Enforce TLS or use Opportunistic TLS (The connection will be encrypted when TLS will be requested and can be negotiated. If TLS is not requested or can't be negotiated it will use plain SMTP)
      * We enforce TLS between our Exchange servers and Mimecast; and we use Opportunistic TLS between Mimecast and outside servers.
  + **Summary or Digest Emails to End Users**
    - Yes, these are sent daily by Mimecast and you can customize when (time of day) they are sent as well as the frequency
  + **Outlook Plug-In**
    - * Mimecast for Outlook (previously Mimecast Services for Outlook or MSO) provides Email Continuity and user access to the features available. These include
        + Email Archive Search
        + Managing Blocked/Permitted Senders
        + Managing messages On Hold
        + Managing/Sending large files
      * Plug-ins for Microsoft Office products can often be a source of instability. We have not experienced compatibility problems with the Mimecast plug-in for Outlook.
        + We have also had a good experience with this add in and our end users like it quite a bit
  + **Login Options**
    - SAML or Single Sign On Options
      * We use Azure AD to populate our directory in Mimecast and then leverage Azure for Single Sign On as well
    - Dual-Factor
      * Two-Factor login is supported
    - Account Synchronization
      * Yes we use Azure AD
  + **Administration and Management**
    - * I find that their Knowledge Base is a worthy first stop. It has a lot of step-by-step articles that are pretty thorough.
      * If additional help is needed, their phone support is great.
      * Mimecast has recently revamped their administration interface. It now is very intuitive. The previous interface could be confusing.

**Advanced or Optional Functionality**

* + **URL Protection**
    - * Targeted Threat Protection – URL Protect is an add-on module at additional cost.
      * Mimecast’s Description: Mimecast Targeted Threat Protection – URL Protect is an advanced email security technology that protects employees against targeted attacks in email, extending our existing Secure Email Gateway anti-spam and anti-virus services:
        + Comprehensive protection, drawing on Mimecast’s threat intelligence infrastructure.
        + Real-time, on-click, every click URL scanning.
        + Instant protection across all devices.
        + Dynamic user awareness helps develop a mentality of employee caution
        + No need for additional infrastructure or IT overhead.
        + Rapid deployment, with single console management and reporting
      * We have had good user acceptance of the URL protect module. Initially we set it up to just warn the user and notify admin. It quickly became obvious that the warning was not sufficient. Within a week, we went to full blocking of dangerous URLs. We have had only one false positive reported since we started blocking.
  + **Advanced File Attachment Defense (sandbox detonation)**
    - * Targeted Threat Protection – Attachment Protect is an add-on module at additional cost
      * Mimecast’s Description: Mimecast Targeted Threat Protection – Attachment Protect is an advanced email security technology that protects employees against targeted zero-hour attacks in email that use weaponized attachments to evade traditional security measures.
        + Flexible attachment protection options allow administrators to choose the best mix of safety, performance and functionality.
        + Pre-emptive sandboxing security checks attachments before they are delivered.
        + Attachment conversion with on-demand sandboxing means safe attachments are delivered without traditional sandboxing delays, helping maintain employee productivity.
        + Instant protection across all devices.
        + Granular reporting allows for end-to-end, real-time threat analysis.
      * We use the Pre-emptive Sandbox mode.
        + Pre-Emptive Sandbox analyses all vulnerable file types in the Pre-emptive Sandbox before delivering the mail and attachments to the user. This does slow down delivery a bit, but we feel that it provides a high level of protection with minimal impact on the user. Attachment conversion has faster delivery, but the user is presented with a PDF of the original document. In some environments tis might be acceptable, but in the case of a collaborative exchange on a document, this would create a lot of confusion, especially if using Track Changes

We do pre-emptive sandbox as well and it has works great for us

* + **Large File Transfer**
    - * Mimecast Large File Send is an add-on module at additional cost
      * Mimecast’s Description: Mimecast Large File Send allows employees to send and receive files up to 2GB in size and stay true to corporate policy without putting a burden on your infrastructure. With Large File Send, file transfer can be controlled by content and archiving policies for searching as well as for e-discovery. Employees simply create an email as usual, attach their file and press send from within Outlook for Windows or a native Mimecast Mac App. Or administrators set policies for attachment sizes and Mimecast does the rest.
      * We subscribe to Large File Send Pro which allows up to 2GB per email with a maximum of 30 GB per month per user.
      * LSF sends a link to the recipient that allows then to download the file via an https session.
      * LFS is accessible in 2 different ways. The easiest is to simply attach files as needed. If the combined attachment size exceeds the limit set by the administrator, Mimecast for Outlook will automatically invoke LFS. In addition, the user can access LFS from the Mimecast toolbar on Outlook and attach any file, regardless of size, using LFS. This is useful if you want to verify receipt of the attachment.
        + Charlie – we use this as well and it has worked great for us
  + **Recipient-Specific Message Encryption**
    - * Secure Messaging is an add-on module at additional cost.
      * Mimecast’s Description: With Mimecast Secure Messaging, data never leaves our secure cloud – making it possible to send protected messages even when TLS encryption isn’t an option. Individuals can initiate Secure Messaging directly in Microsoft Outlook for Windows to specify controls, such as whether an email can be forwarded or printed, or when read privileges expire. Policies can be configured to be applied directly at the gateway. All these controls are simple for employees to use and most importantly stop the use of unapproved applications. Mimecast makes it easy for employees to follow corporate security policies and for administrators to enforce them and monitor email compliance.
      * Mimecast Secure Messaging is a feature that requires the recipient to log into the Mimecast Portal to receive their message.
        + Charlie – we use this feature and it works well for us
  + **Data Loss Protection (DLP)**
    - Included in subscription
  + **Email Continuity**
    - * Mailbox Continuity is a core feature of Mimecast (included in the subscription)
      * Mimecast’s Description: With Mimecast Mailbox Continuity downtime is a thing of the past. In the event of a sudden email outage or planned downtime, Mimecast provides uninterrupted access to live and historic email and attachments from the Mimecast Cloud using everyday tools like Outlook for Windows, the web and mobile applications. Employees get guaranteed access to email —from anywhere, on any device. And administrators can do it all without expensive hardware and software.
      * By implementing the Outlook plugin and Archiving, we automatically take advantage of “Continuity Mode”. If Outlook cannot connect to the Exchange server, but does have access to the Internet, it will automatically switch to Continuity Mode. As part of the base Archiving, we have set up Journaling to Mimecast. As a result, Mimecast has the ability to present an inbox that is as up-to-date as the Journaling. We use on-prem Exchange (2013), but according to Mimecast, it will work with hosted Exchange as well.
        + Charlie – We use this as it is part of the core offering. We do not integrate with outlook. We use our Single Sign On page and Mimecast personal portal is an option there. People can just sign in with their domain username and password.
  + **Archiving**
    - Optional at an additional cost

**Support**

* + **SLA’s**
  + **Availability, Accessibility and Responsiveness**
    - * Standard Business Support includes email support plus phone support “during standard business hours”
      * 24/7 phone support is available for an additional charge
      * My experience with Mimecast support has been overwhelmingly positive.
      * Their Knowledge Base is the first stop for me and I can often find the answers there. They have recently announced a new interface they call Mimecaster Central which is very helpful.
        + The Knowledge Base is very solid and a resource I rely on regularly.
      * When contacting support by phone, a technician is nearly always available within minutes. On the rare occasion that they are backed up, the call-back is prompt.
      * I feel that I get expert technical help immediately. They are very knowledgeable on the product.

**Implementation**

* + **Time Required**
    - The implementation process for us was pretty straightforward. The entire process took about a month to complete. We started by routing outbound email through Mimecast which built a list of “safe senders.” As attorneys and staff sent email through the service the recipients were automatically whitelisted. After about 2 weeks we cutover inbound email to close out the implementation.
  + **Complexity**
    - Mimecast has a 7 step implementation process that guides you through the implementation. Each time you complete a step you receive an automated email confirming the step is complete and documentation on how to complete the next step. This really simplified the implementation for us and made it pretty seamless.
  + **Cost**
    - There was no additional cost for implementation.
  + **Support**
    - We were assigned a dedicated implementation engineer who was available to assist if needed as we progressed through the implementation process.
  + **End-User Training**
    - Online training is available for the implementation process. The also was an in depth knowledge base and community forums as a supplemental resource. Additionally, our in house trainer had classes that corresponded with our implementation to educate our users on the ins and outs of the Mimecast platform.
  + ***Administrator Training***
    - Implementation engineer was available to answer questions. Also there was online training, knowledge base and webinars available as a supplemental resource.