**ProofPoint Features Breakdown**

By Holt Satterfield and Mike Viscito

**Core Functionality**

* + **Spam Filtering**
    - ProofPoint uses multiple sets of criteria to score messages, stopping 99% of spam.
    - In our experience, spam filtering has been very effective by ProofPoint.
    - That said, periodically SPAM does get through, allegedly because it does not yet exist in ProofPoint’s database. These are then to be submitted to ProofPoint to have signatures created against them.
  + **Additional Content Filtering (Objectionable material, customized rules, etc.)**
    - Built-in categories to filter for material like adult content.
    - Additional custom options to create your own rules to filter specific senders, text, file attachments, etc.
  + **File Attachment Screening (Traditional Signature Based AV)**
    - Multi-layer attachment filtering promising 100% virus protection.
  + **Impersonation Protection (SPF/DKIM/etc.)**
    - SPF, DKIM and DMARC (combining SPF and DKIM) Filtering is part of the base ProofPoint product.
    - Some external senders you may want to be approved to send to an internal recipient, but not one you’d want to include in your own SPF records. For those a bypass rule will need to be created.
    - This portion I’d recommend spending time on specifically with the implementation engineer prior to deployment.
  + **Phishing Defense**
    - Included in Impersonation Protect
  + **Email Server to Email Server Security (TLS Support)**
    - ProofPoint has the ability to use either Enforced TLS or Opportunistic TLS on a per-domain basis.
      * In Opportunistic TLS, ProofPoint always uses TLS security for email if the other mail system supports it, but if not it will fall back to unencrypted SMTP.
      * In Enforced TLS, ProofPoint ONLY sends emails if a secured TLS connection can be established. If that’s not possible for some reason, it will not delivery the email and result in a non-deliverable report to the sender.
    - We use Enforced TLS between our Exchange servers and ProofPoint.
    - We use Enforced TLS for security between the ProofPoint and our clients on an as-requested basis.
  + **Summary or Digest Emails to End Users**
    - These are sent on a schedule the customer determines to their end users. We send them once per day. Schedules can be customized to different groups of people at different times of day or even sent multiple times per day.
    - The digest only displays quarantined emails for the past 24-hours (or since the last Digest was received).
    - Within this digest email are several links:
      * to generate a new digest should the user desire a current quarantine list.
      * to release instantly any of the displayed captured emails.
      * to release instantly and white-list any of the displayed captured emails
      * to mark any of the displayed captured emails as Not Spam.
  + **Outlook Plug-Ins**
    - Outlook plugin for quarantine inspection and feedback on message spam scores. We do not currently use this plugin however because the functionality it offers does not outweigh the additional maintenance and stability issues additional Outlook plug-ins generate.
    - Outlook plugin for Email Continuity
    - Outlook plugin for Encryption
    - Outlook plugin for Large File Send
  + **Login Options**
    - SAML or Single Sign On Options
      * ProofPoint offers the option to use SAML based authentication for end user authentication.
    - Dual-Factor
      * Dual-factor authentication is not natively offered with ProofPoint but with SAML auth could be integrated at your SAML provider.
    - Account Synchronization
      * We use an on premise install of the ProofPoint appliance to synchronize account information from Active Directory.
  + **Administration and Management**
    - * Web UI for policy management
      * Can appear fairly complex when you first step into it. The time with the implementation engineer is well spent here to review all the different modules and the ways in which they interact.
      * I’d also recommend a full review of order of operations and where overrides are so you have a full understanding of what portion to administer to have the effect you desire.
      * After deployment our internal administrators were fairly self-sufficient.

**Advanced or Optional Functionality**

* + **URL Protection**
    - * Included in the Targeted Attack Protection module offered at additional cost.
      * URL’s on inbound messages are examined by ProofPoint. They are re-written to force any clicks through ProofPoint.
      * URL’s deemed harmful by ProofPoint will be blocked on any endpoint the user attempts without any local software installation, so it truly follows the user anywhere.
      * In our experience, some trusted URL’s have been added to a bypass policy because of issues with the way a local application deals with the re-written URL. These are very rare.
  + **Advanced File Attachment Defense (sandbox detonation)**
    - Included in the Targeted Attack Protection module offered at additional cost.
    - Attachment defense will open the email attachment in a virtual machine and will observe the behavior after the attachment is opened. It will look for any suspicious behavior (new processes, new registry entries, etc.).
    - When attachments arrive, ProofPoint first checks the digital fingerprint of this attachment against a list of known threats it previously identified via sandbox detonation. If it’s seen this file before on any customer’s system and it’s been flagged, it will stop the attachment immediately from being delivered. Every customer protected by this product helps anonymously add to the known threat list by having this feature enabled. Only the hash of known threats is kept in the list keeping any contents of suspected file attachments completely secure to each customer.
    - If it has not yet seen this attachment it opens the attachment in a virtual machine and then looks for any suspicious behavior.
    - The system can be configured to wait for this scan to take place (which can take varying amounts of time depending on the attachment size) or it can be configured to deliver immediately to the recipient.
    - If you choose to deliver immediately to the recipient an alert can be configured to your internal Security and Email teams to alert them that a threat has been found on a delivered attachment.
    - When enabling this feature you need to decide if immediate receipt of emails is more important than this level of inspection for threats. This can be very effective against zero-day or frequently mutating attacks delivered via file attachment.
    - One effect of requiring all files to be scanned before delivery could be emails in a thread appearing out of order. For example, if emails 1,2,3 are sent, and email 1 contains a large attachment but 2 and 3 do not, emails 2 and 3 may be received before email 1 although it was authored first. Additionally, other parties to an email may receive a copy of the email and attachment before the user you’re protecting.
    - You can choose to tier different levels of protection based on job function, for example requiring full scans to complete for staff and assuring immediate delivery for fee-earners.
  + **Large File Transfer**
    - Offered in two flavors as an add-on module at additional cost:
      * 2GB file send from within Outlook.
      * 5GB file send from a web-hosted site.
  + **Recipient-Specific Message Encryption**
    - Data Loss Prevention and Privacy is an add-on module at additional cost.
    - ProofPoint can encrypt email, requiring recipients to click a link and open a web interface over SSL before retrieving the contents of the message.
    - A copy of the email can optionally be downloaded by the recipient once they’ve authenticated to the web page, providing flexibility on the recipient’s end for storing the email in systems like DMS.
    - This may be useful in cases where you’re required to encrypt email down to the individual recipient level but do not want to manage X.509 certificates for traditional recipient-level encryption.
  + **Data Loss Protection (DLP)**
    - Data Loss Prevention and Privacy is an add-on module at additional cost.
    - ProofPoint has built-in patterns to search for common DLP concerns like PHI, PCI, PII.
    - Custom rules can be created to filter for additional criteria in messages.
    - Different actions can be taken when a DLP rule is triggered, including notification to sender or others (like Security and Risk teams), approval requests by others in your organization before sending, message rejection and forced recipient level encryption.
  + **Email Continuity**
    - Neither reviewer has used this module in production, so the information here is based on what is provided by ProofPoint.
    - Up to 30 days of externally sent/received email is available within Outlook clients or via a web interface.
    - Further details available here:  
      https://www.ProofPoint.com/sites/default/files/ProofPoint-enterprise-continuity-data-sheet.pdf
  + **Archiving**
    - Neither reviewer has used this module in production, so the information here is based on what is provided by ProofPoint.
    - “Information Archiving” is available as an additional service by ProofPoint and is intended to replace on-prem archival solutions and remove the presence of PST’s in your environment.
    - Further details available here: https://www.ProofPoint.com/us/products/information-archiving

**Support**

* + **SLA’s**
    - Are available
  + **Availability, Accessibility and Responsiveness**
    - ProofPoint just upgraded their Customer Service interface and process, which has been a negative cited by Administrators
    - Issues need to be entered into a Support web-interface, along with any relevant attachments.
    - Unless the issue is Priority One (outage), the response time can lag
    - Support quality is very good

**Implementation**

* + **Time Required**
    - Sufficient time needs to be given to identify customized portions of your existing solution and mapping those to ProofPoint equivalents. You also need to plan to educate your users on the new interface and process. We moved to ProofPoint from Postini and the process was fairly painless. I’d say a month of focused time for the Email administration team would be sufficient.
  + **Complexity**
    - A PM works with you from ProofPoint to help manage the transition. It does take some time to identify all the custom rules or settings you may have on your current solution and map those to ProofPoint, but we were very happy with the technical resource from ProofPoint that helped manage that process.
  + **Cost**
    - There was no additional cost for implementation. Overall cost of the ProofPoint solution can be expensive, especially when adding in the optional modules.
  + **Support**
    - The technical resource that served as our PM through the process was very responsive during implementation.
  + **End-User Training**
    - We were able to take material from ProofPoint and use that as a starting point for our training team. Quick Reference Guides and email campaigns were used, but we never offered classes to explain the transition.
  + ***Administrator Training***
    - Time spent with the implementation engineer was very valuable as it helped us get acclimated to the new system with minimal disruption. During the migration and deployment phases we leaned on them heavily but that decreased over time and we found ourselves largely self-sufficient. That said, unless in-house technical resources are dedicated to ProofPoint, a smaller office might find it necessary to continue to seek ProofPoint for management assistance