clearswift
by HelpSystems

SOLUTION BRIEF *(Cybersecurity)*

Using Clearswift Secure Email Gateway to enhance data security in Microsoft Office 365

For many organizations, Office 365 is the ideal collaboration tool, providing a convenient platform for employees to share information and communicate daily. Microsoft offers different tiered packages to suit a variety of customer requirements. Its Office 365 Enterprise E5 and Microsoft 365 E5 packages provide platforms for mid and larger sized enterprises, with lower tiered products offering fewer inclusive features and therefore less protection against ransomware, advanced persistent threats (APT) and data loss protection (DLP) risks.

In this document, we look at the common areas of concern we hear from customers using the Office 365 Enterprise E5 and Microsoft E5 platforms and look at how the Clearswift Secure Email Gateway (SEG) can be used to provide enhanced Adaptive Data Loss Prevention (A-DLP) protection and complement the Office 365 hygiene components.

More Comprehensive and Easier to Configure Adaptive DLP and Compliance Controls

The Office 365 Enterprise E5 and Microsoft 365 E5 tiers offer the Information Protection and Compliance feature as part of the subscription, whereas it is an additional cost option for the M3 tier.

One of the key areas of feedback from our customers is that the DLP controls within Office 365 are less than comprehensive and can be hard to configure effectively (e.g. pre-configured GDPR policy controls only cover German, UK and USA PII data).

Key areas of concern with Office 365 DLP controls are:

- DLP policies are time consuming to create and it is difficult to build sensible levels of granularity into the policy (e.g. block all reports from Child Protective Services from going to inappropriate people inside/outside the organization, but still allow those internal/external recipients to receive the relevant information in a secure format)
- Understanding what DLP policies apply to users/groups of users can be time consuming and can lead to inadvertent gaps in policy
- Unable to detect sensitive information (e.g. PII and PCI data) within image files and scanned documents which creates a risk of GDPR violations
- Based on "stop and block" principles requiring manual intervention, which has a direct impact on resources and productivity.

By deploying the Secure Email Gateway alongside Office 365, customers can benefit from:

- Easier to configure and manage DLP controls, which allow the organization to configure a DLP policy that supports existing business processes, rather than asking users to change their behavior to suit the less flexible controls within Office 365
- Adaptive DLP controls to remove business risks without blocking communications unnecessarily
  - » *Data redaction of common office documents (e.g. Adobe PDF, Microsoft Word, etc.) and email messages to remove sensitive data (e.g. PII, PCI, etc.)*
  - » *Document sanitization of common office documents (e.g. Adobe PDF, Microsoft Word, etc.) to automatically remove document properties, tracking information and previous versions*
  - » *Anti-steganography functionality to prevent exfiltration of sensitive information within image files*
- Optical Character Recognition (OCR) functionality to detect sensitive information (e.g. PII and PCI data) within image files and scanned documents and reduce the risk of GDPR violations
- Policy-based encryption using PGP, S/MIME, Password and Portal to offer a greater range of encryption options when communicating with different audiences
- Integration with the Clearswift Information Governance Server to provide more comprehensive DLP controls around forms and image-based data (e.g. Child Protective Services case reports, etc.)
  - » *Offers full and partial document fingerprinting and data classification, which means that a paragraph of text and an image copied from a classified document and pasted into an email will still be recognized as classified information and blocked from being shared with inappropriate recipients.*

Please note that some of the above features are additional cost options.

All of the Secure Email Gateway Adaptive DLP policies can, of course, be enforced on emails entering and leaving the organization. However, SEG can also extend these controls to emails circulating within the organization, which has allowed a number of our customers to address the risk of information being shared with inappropriate recipients within their own organization (e.g. a member of the Child Protective Services team accidentally choosing the wrong group in Outlook and emailing some case reports to senior managers within the organization).

Additional Layer of Ransomware and APT Protection

Another reason our customers deploy the Secure Email Gateway alongside their Office 365 instance is to provide an additional layer of protection against phishing, ransomware and APT attacks.

Our recommended best practice to ensure that you have adequate defenses in place to thwart phishing, ransomware and APT attacks, is to not only use multiple layers of defense, but also multiple methods of protection. The M5 and E5 tiers offer the ATP feature which incorporates Safe Attachments and Safe Links (checks reputation of hyperlinks). This ATP feature is also available as an additional cost option for the M3 tier. However, one of our customers' key concerns is that this ATP feature alone does not provide them with the certainty of protection that they require against ransomware and APT threats. If an attacker understands how the ATP feature works, then they can craft an attack that will appear innocuous in order to bypass the ATP feature and then become active once the user opens it at their desktop. In addition, an attacker can easily sign up for an Office 365 account and test their attacks against that, before moving onto their real target once they know that they have crafted an attack that bypasses the Safe Attachments functionality.

The Secure Email Gateway offers an alternative approach that complements the APT functionality in Office 365, without unnecessarily delaying legitimate business communications. Using SEG, our customers can strip the active content from common office document formats (e.g. Adobe PDF, Microsoft Word, etc.) and deliver the sanitized underlying data through to their users. This approach removes the active content that is commonly used in successful ransomware and APT attacks and because it removes all of the active content, then there is no ability to fool the defenses.

The active content sanitization is offered in addition to more traditional layers of protection, such as:

- Anti-spam controls
- Multiple anti-virus options
- File type controls (e.g. executable file types, script files embedded within compressed file formats, etc.)
- Anti-steganography to remove APT threats hidden within image files.

Better Visibility of Policy Violations and Tracking of Message Flow

Customers have also told us that the reporting functionality in Office 365 is fine for day-to-day mail flow management tasks but is somewhat lacking when trying to investigate DLP policy violations. This is exacerbated when the users that need to perform the investigations are non-technical (e.g. HR, Compliance, etc.).

The Secure Email Gateway provides a level of visibility for policy violations that is much easier to understand and enables deeper investigation into the root cause of the violation. Better visibility is provided both at the reporting level and within the inform messages sent to key personnel within the organization (e.g. HR, compliance, the perpetrator’s manager, etc.).

Another reason our customers cite for using the Secure Email Gateway alongside their Office 365 deployment is that they find the message tracking functionality on SEG superior to the functionality offered by Office 365. SEGs message tracking:

- Is much easier to use
- Provides real time visibility of message flow
- Allows for rapid diagnoses of how a message was processed and what happened to it.

This allows operational teams to respond to user support queries about emails sent/received in real time with absolute certainty as to what has happened.

Additional Benefits

In addition to these long-term benefits, one of the areas where we have seen customers benefit from this multi-layered approach is during the migration from on-premise Exchange to Office 365 itself. Clients that have a mixture of on-premise (e.g. internal applications sending emails out, third parties routing emails through their organization on their behalf, etc.) and Office 365 report that they have found it much simpler to configure email routing at the Secure Email Gateway level, rather than in Office 365.

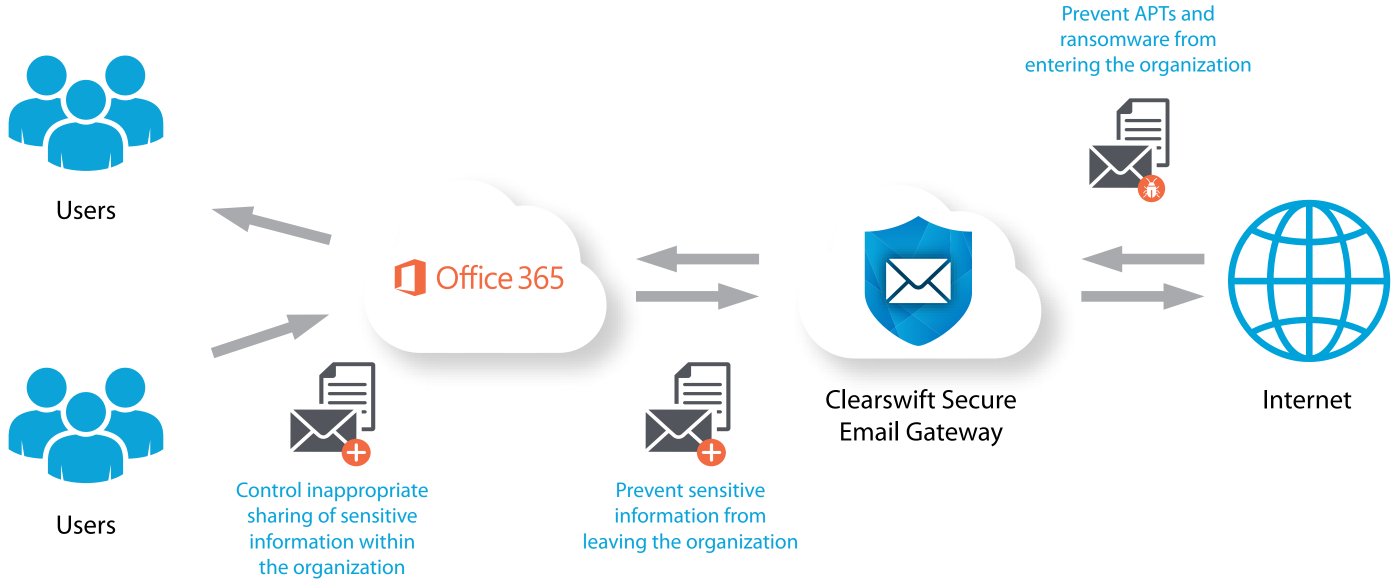
In Summary

Clearswift Secure Email Gateway complements Office 365 in three ways:

1. It offers more comprehensive and easier to configure Adaptive Data Loss Prevention (A-DLP) and compliance controls that removes the risk without unnecessarily blocking communication.
2. It provides an additional layer of ransomware and Advanced Persistent Threat (APT) protection, using multiple layers of defense and multiple mechanisms to reduce risk and combat zero-day targeted attacks.
3. It affords better visibility of policy violations, allowing teams to gain a deeper, more timely understanding of policy violations and tracks message flow in real time.

The Secure Email Gateway can be deployed on-premise, in the cloud (e.g. Microsoft Azure and Amazon Web Services), or as a managed service in front of a customer's Office 365 deployment. Once deployed, it scans all:

- Inbound email traffic
- Outbound email traffic
- Internal email traffic


Prevent APTs and ransomware from entering the organization
Users
Office 365
Users
Clearswift Secure Email Gateway
Internet
Control inappropriate sharing of sensitive information within the organization
Prevent sensitive information from leaving the organization

Features Table – Better Together

Functionality	Office 365	Secure Email Gateway	Secure Email Gateway and Office 365
Anti-virus	✓	✓	✓
Anti-spam	✓	✓	✓
Stop and block policy enforcement	✓	✓	✓
Isolation sandboxing	✗	✗*	✗*
Active content sanitization to protect from ransomware and APTs	✗	✓	✓
Stop and block DLP controls	✓	✓	✓
Adaptive DLP	✗	✓	✓
Data redaction	✗	✓	✓
Automated Document Sanitization of metadata and version history	✗	✓	✓
Anti-steganography	✗	✓	✓
Optical Character Recognition (OCR)	✗	✓	✓
B2B encryption	✓	✓	✓
B2C encryption	✓	✓	✓

*Coming soon

Find Out More

Discover more about our Secure Email Gateway, ask for a demo at www.clearswift.com.

clearswift
by HelpSystems

www.clearswift.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.