clearswift

A HelpSystems Company

Enhancing Information Security in Microsoft Office 365

With Advanced Content Inspection & Data Security Features

Table of Contents

Enhancing Microsoft Office 365 With Advanced Security Features

Microsoft Office 365 has certainly captured the corporate imagination. The cloud software suite offers organizations a mass of business collaboration improvements and depending on the Tier level deployed, significant cost savings from both technology and operational overhead standpoints. It also has built-in email security features that have seen many organizations move away from dedicated email security solutions and subsequently, the teams that manage/administer them, as part of a migration over to the Cloud platform.

But, does Microsoft Office 365 deliver the advanced levels of cyber-attack prevention and information security that is required in today's digital age?

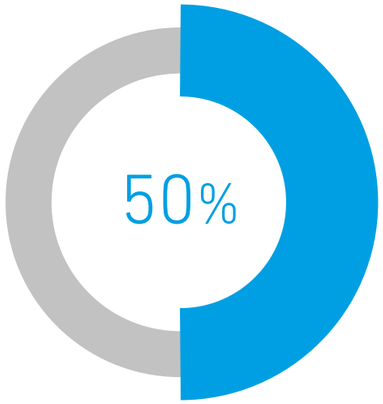
While most organizations might initially think so, it is often not realized until after migrating to the cloud environment that information security within the platform is nowhere near the level they might previously have been used to. In fact, the basic security features offered in Microsoft Office 365 compared to those associated with a dedicated email security solution are vast. With cyber criminals becoming increasingly creative with delivery methods of sophisticated threats, as well as data protection laws become tighter, organizations that store and process highly sensitive information in Microsoft Office 365 need to weigh up both the benefits of platform, and the cyber risks associated with it.

Clearswift offers a solution that seamlessly integrates with Microsoft Office 365 to enable advanced threat protection and data protection features that close security gaps within the platform to mitigate risks. The level of protection is enhanced to prevent sophisticated attacks and data breaches is occurring.

Critical Information in the Cloud

Cloud suites and applications continue to cause concern for IT security professionals who see them as a potential catalyst for end users to operate beyond the jurisdiction of the IT department.

Within an independent survey, research consultancy Loudhouse asked IT decision makers about their worries about internal security threats. The cross-sector response was consistent: More than 50% said the use of cloud applications beyond the IT department's control was a concern, and more than 10% said it had already, directly or indirectly, caused a security breach in their organization.



More than 50% said the use of cloud applications beyond the IT department's control was a concern

How Office 365 security stacks up

If you are an Office 365 customer, you are automatically protected by an anti-virus and anti-spam service. The level of protection depends on the package. While it comes with all the benefits of a hosted service with financially-backed SLAs, there are some concerns.

- Data loss prevention controls 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).
- Unable to detect sensitive information (e.g. PII data) within image files and scanned documents
- Unable to remove data loss and malware threats hidden within image files
- There can be a delay in the application of outbound mail policy changes that you make to the service
- Does not provide a means to quarantine outbound email; only reject, sender release override or redirect to administrator
- Can only block file types (by signature)if they are 'executable'
- Limited number of notification options (sender, recipient or admin)
- No re-use of existing lists (profanities, expressions)
- No means to duplicate rules, forcing new rules to be created from scratch with different rule criteria (e.g. sender or recipient or violation action)
- Complex customer configurations may make managing policy difficult
- Spam policy appears to only have a single default setting, so enabling the source and language settings could be disastrous in a multinational organization
- Unable to define new custom file format types (by signature)
- Unhelpful or misleading error messages
- Reporting does not provide the level of comprehensive but easy to understand detail required to investigate an information security breach

It's all about content

Email is considered the second most common source of data leakage after removable storage. Forrester estimates that one in five emails contains data that presents a legal, financial or regulatory risk. You need to be sure that your security tools will scan deep into the message and any attachments to identify any critical information before it leaves the organization.

Office 365 is good for dealing with spam and malware and does offer organizations a basic level of email security, such as tools to deal with regulatory control through archiving and basic encryption. Template rule sets are provided to get you started with policies, but these typically do not provide the deep content inspection required to remain secure as an organization and may also be subject to additional charges.

A zero compromise enterprise

Through implementing Clearswift technologies, in conjunction with the benefits provided by your Office 365 implementation, you will have the missing piece of the security structure you ultimately require. And, with the additional benefits of Adaptive Redaction you can be sure that your organization's critical information remains secure within the Office 365 framework in the knowledge that your organization won't have to compromise collaboration for security.

The Clearswift SECURE Email Gateway covers these bases comprehensively. Its Deep Content Inspection engine deals with message headers, senders and recipients, subject lines, message bodies, attachments and contents, image scanning, document headers and footers, and even meta data accompanying documents.

This maximizes the chances of capturing sensitive content such as credit card numbers and banking codes, confidentiality clauses and profanity, as well as customer-defined and regular expressions, and Boolean and positional operator-based expressions.

Furthermore the solution can be used to monitor and control internal email, providing granular controls and advanced DLP functionality to prevent unauthorised data sharing within the business. While organizations control access to file servers and other collaboration services, recognising the fact that not all information should be available to all people, internal email traditionally has no such restrictions. Allowing anyone to send anything to anyone else inside the organization. This creates risk which can be prevented using the SECURE Email Gateway.

The adaptive enhancement to Office 365 security

If you are an Office 365 for Enterprise Customer, and concerned about the security of your organization's critical information or sensitive data that exists within this environment, it would make sense to introduce the adaptive data loss prevention technology, only available from Clearswift:

- Granular policy rules from senders, recipients, domains and departments
- Policy applicable to inbound, outbound and internal emails
- Full and partial document fingerprinting and classification
- Optical Character Recognition (OCR) functionality to detect sensitive information (e.g. PII, PCI, etc.) in images and scanned documents
- Adaptive Redaction functionality*
  - Data redaction of Word, Excel, PowerPoint, PDF files and email messages to remove sensitive data (e.g. PII, PCI, etc.)
  - Document sanitization (including Tracking and Property removal)
  - Structural sanitization of documents to remove active content and other potentially malicious components from files such as APTs, ransomware, etc
  - Anti-steganography functionality to prevent exfiltration of sensitive information within image files and strip incoming embedded threats
- Policy-based encryption using PGP, S/MIME, Password and Portal
- A simple configuration of rules for different users and groups policies, especially with lots of rules to apply to different user group combinations
- A customizable 'Missing Manager' policy, which allows an administrator to define a manager for each user and inspects CC and TO fields for their email address
- The ability to define custom file type detection to block files that are too sensitive to rely on extension based controls
- The ability to save a copy of policy or rollback to a previous one if a change doesn't do what you expected

Clearswift offers a more comprehensive, secure solution than a hosted option alone - a must for any IT security professional, balancing critical information protection and control with an increasingly cloud-centric infrastructure.

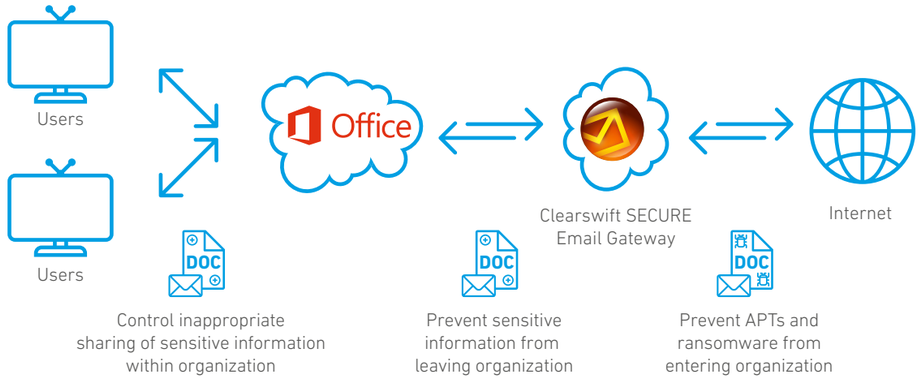
* standalone Adaptive Redaction functionality can be implemented into any environment with ARgon for Email

Integrating Office 365 with the Clearswift SECURE Email Gateway or ARgon for Email

Clearswift can be deployed alongside Office 365 in a number of ways, ensuring that the information that is of most value to your organization remains secure - wherever it resides, even in the 'cloud':

1. Can scan inbound email traffic
2. Can scan outbound email traffic
3. Can scan internal email traffic
4. Management of web traffic - required if using browser based client for mail access
5. As a hybrid configuration (where organizations are using both Office 365 and an on-premise email solution)
6. Can manage end point security - although Office 365 has Sharepoint management, further egress points such as USBs, external storage, etc. need to be managed to ensure critical information protection

Microsoft Office 365 offers a comprehensive hosted email and Sharepoint solution, with a good, but basic security offering. However, for today's Enterprise to have confidence that their critical information is secure and that their most valuable or sensitive data will not be subject to a breach - enhancing that functionally with an adaptive approach to security is the only viable option.



clearswift

A HelpSystems Company

Clearswift is trusted by organizations globally to protect critical information, giving teams the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations' to have control to gain visibility and control of critical information 100% of the time.

For more information, please visit **www.clearswift.com.**

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading
RG7 4SA
UK

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Hub Hyde Park
223 Liverpool Street
Darlinghurst
Sydney NSW 2010
AUSTRALIA