TECHNICAL DOCUMENT

| | |
|---|---|
| *Reference Nr.* | 20190211/SD/1 |
| *Written by* | Spiros Delimpasis |
| *Latest update* | 2019-02-27 |
| *Comments / Applies to* | Clearswift SECURE Email Gateway<br>Microsoft Office 365 |

# Compare Office 365 to Clearswift SECURE Email Gateway

**Microsoft Office 365 is gaining in popularity among organizations worldwide, regardless their size. The cloud-based service allows the IT Department to cut down on infrastructure costs, while enabling users to access their mailbox from everywhere. The benefits of Microsoft Office 365 in providing a comprehensive collaborative software and communications suite are indisputable. This document focuses on the security features provided by Microsoft and why it is still essential for an organization to deploy the SECURE Email Gateway in front of the online version of Exchange.**

All Office 365 customers 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:

- There can be a delay in the application of outbound mail policy changes
- It does not provide a means to quarantine outbound email. The only available actions are "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, lexical 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 policy management 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 is poor with either reports failing to be generated or timed out

Negreponti 5
413 35 Larissa, Greece
Tel. (+30) 2410-670030
Fax.(+30) 2410-670006
email sales@inter-datasecurity.com
URL: www.inter-datasecurity.com

While the **hygiene controls** of Office 365 are considered good, they cannot perform well in targeted attacks. The traditional AV part of the solution uses signature-based and heuristic detection methods, which advance APTs can readily bypass.

**Information protection policy** is limited and not adaptable enough. It is considered very US centric, it either allows or blocks the transmission of a message and it can be very time consuming to create and manage granular policies. All in all the service does not offer depth of detection and flexibility of definition, so risks go undetected, or false positives impose management overhead.

Experience, mirrored by anecdotal discussions with partners, is that a significant proportion of organizations that move to Office 365 and drop traditional boundary email solutions in the process, return within 12 months as they realize that Office 365 does not offer them the full range of defenses to mitigate the variety of information risks that a modern organization faces.

Office 365 offers email archiving services by using legal hold, which is implemented either with Litigation Hold on In-Place Hold. Each method offers different features but both of them have limitations.

- Litigation Hold must be enabled permanently to prove a message has not been tampered.
- Accidental user deletion can lead to loss of mailbox and its content, even when archiving is enabled.
- Increased cost because mailbox of users that leave the organization cannot be deleted.
- If archiving is disabled for a mailbox, all messages older than the retention period will be lost.
- Degradation of search performance as number of mailboxes increase (no SLA for search times)
- Search results limited to 200

Office 365 can only Journal to an External Address, for the purposes of enabling use of 3rd party journal archive technology. Without such a 3rd party service it is not possible to:

- Access any of the emails on Litigation Hold and/or Live email if O365 goes down
- Prove that an email has NOT been sent or received (without Litigation hold set permanently on for ALL mailboxes that have ever existed in the organization)
- Have tamper evident email (without Litigation hold set permanently on for ALL mailboxes that have ever existed in your organization)

## Clearswift SECURE Email Gateway feature set

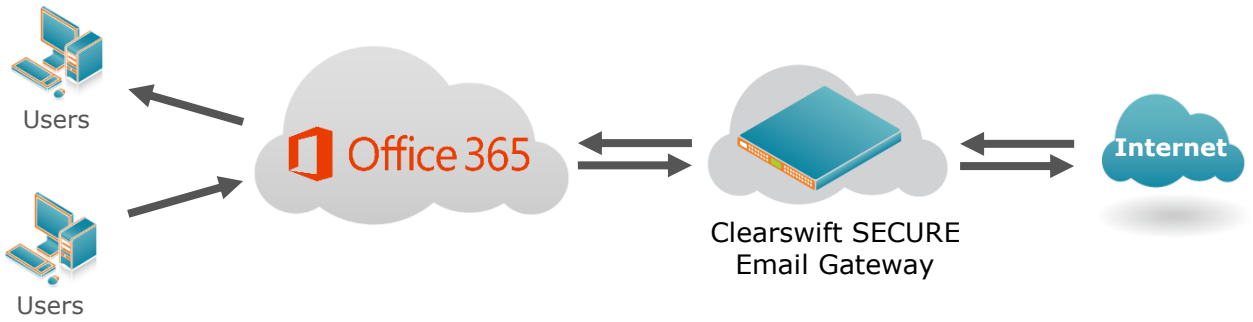
Clearswift SEG can be deployed to scan inbound and outbound emails in order to secure Office 365. The key features are:

- Granular policy rules from senders, recipients, domains and departments
- Adaptive Redaction functionality
    - Data redaction of Word, Excel, PowerPoint, PDF files and email messages to remove sensitive data
    - Document sanitization (including Tracking and Property removal and removal of embedded content in images)
    - Structural sanitization of documents to remove active content and other potentially malicious components (such as APTs) from files
- 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
- A web portal that users can login to view and manage their quarantined messages
- MIME type detection based on hexadecimal signatures
- 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
- OCR to apply content inspection in images
- 60+ configurable reports

**Deployment options**

SEG can be deployed in a physical machine or in a virtual machine in the organization premises. It is also possible to install it in Azure or AWS.




**Email Archive Addon**

Clearswift SEG does not offer email archiving as a standard feature, but it integrates with Cryoserver Email Archiving. Key features of the addon service are:

- Emails are journaled in real time
- Mail Server agnostic
- Stored emails are tamper-evident and court-admissable
- Searches quickly and accurately
- Meets sector-specific regulations, data privacy & human rights legislation
- Facilitates policy-based access rights and role-based access
- Maintains tamper-evident audit trail
- Searches millions of emails in seconds
- Slashes time and cost of eDiscovery, SAR and other formal searches
- Limits IT Department involvement in finding lost email
- Assists migration to new mail servers
- Reduces server management costs
- Cuts premium storage costs on the mail server
- Enables email usage even when the mail server is down
- Empowers end users with intuitive, super-fast search screens
- Seamless integration with Outlook
- Combines searches for more accurate and refined searches
- Replicates user's Outlook email folders within the Cryoserver interface
- Accesses emails remotely via Cryoserver Mobile App (iOS, Android, Windows & Blackberry)

Cryoserver can be delivered on premise (software or prebuilt appliances), in the cloud or as Managed Service Provider.

## Conclusion

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. An organization needs to be certain that security tools will scan deep into the message and attachments to identify any critical information before it leaves the business.

Office 365 is good for dealing with spam and malware and does offer organizations the basic email security but does not provide the deep content inspection required to remain secure as an organization and may also be subject to additional charges. Through implementing Clearswift SEG, in conjunction with the benefits provided by Office 365 implementation, an organization will have the missing piece of the security structure ultimately required. The additional benefit of Adaptive Redaction can ensure that critical information remains secure within the Office 365 framework.



Negreponti 5
413 35 Larissa, Greece
Tel. (+30) 2410-670030
Fax.(+30) 2410-670006
email sales@inter-datasecurity.com
URL: www.inter-datasecurity.com

Inter Engineering®
World of Data Security!