

SEG vs Office 365 Security Features

Feature outline

July 2017

Copyright

Published by Clearswift Ltd.

© 1995–2017 Clearswift Ltd.

All rights reserved.

The materials contained herein are the sole property of Clearswift Ltd unless otherwise stated. The property of Clearswift may not be reproduced or disseminated or transmitted in any form or by any means electronic, mechanical, photocopying, recording, or otherwise stored in any retrievable system or otherwise used in any manner whatsoever, in part or in whole, without the express permission of Clearswift Ltd.

Information in this document may contain references to fictional persons, companies, products and events for illustrative purposes. Any similarities to real persons, companies, products and events are coincidental and Clearswift shall not be liable for any loss suffered as a result of such similarities.

The Clearswift Logo and Clearswift product names are trademarks of Clearswift Ltd. All other trademarks are the property of their respective owners. Clearswift Ltd. (registered number 3367495) is registered in Britain with registered offices at 1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England. Users should ensure that they comply with all national legislation regarding the export, import, and use of cryptography.

Clearswift reserves the right to change any part of this document at any time.

Contents

Feature Comparison 4
Office 365 Notes 5

Feature Comparison

This document provides a simple comparison of features between the SEG and Office 365 platform.

Feature	Clearswift	Microsoft
Deployment Models	5	1
Appliance	✓	✗
Virtual Appliance	✓	✗
SaaS	✓ *Regional	✓
Hosted	✓	✗
Managed Service	✓	✗
Malware protection (engines)	2	3
Own	✗	✓
Third Party	✓	✓
Sanitize Body	✓	✗
Sanitize Attachment	✓	✗
Open Source AV	✗	✗
Sandbox	✗ *Soon	✓
Anti-Spam	Yes	Yes
Own	✓	✓
Third Party	✓	✓
Multiple vendors	✗	✓
Real time URL lookup	✓	✓
URL removal	✓	✓
Domain Authentication Methods	SPF/DKIM/DMARC	SPF/DKIM/DMARC
Open Source AS	✗	✗
Image Detection	Yes	No
Image spam	✓	✗
Image content inspection	✓	✗
True File Detections	Yes	Yes
Extension	✓	✓
File signature	✓	✓
Create custom extensions	✓	✗
Rich Keyword Search	Yes	Yes
Subject	✓	✓
Message body	✓	✓
Attachments	✓	✓
Data Sanitization	✓	✗
Data Redaction	✓	✗
Full / Partial fingerprint	✓	✓
Supplied patterns	100+	80+
Regular expressions	✓	✓
Further DLP Features	Yes	Yes
Separate areas for different violations	✓	✗
Pre-built Dictionaries	✓	✓
Pattern Matching	✓	✗
Endpoint DLP	✓	✗
Encryption	Yes	Yes
TLS	✓	✓
Password	✓	✗
Push/Pull	✓	✓
S/MIME	✓	✗
PGP	✓	✗
PDF	✗	✗
Records Management	✗	✓
IBE	✗	✗
Reporting	Yes	Yes
Advanced Capabilities	Yes	No
Email Archiving	✓ 3rd Party	✓
Email Continuity	✓ 3rd Party	✗
End User Mail Management	Yes	Yes
Digest	✓	✓
Portal	✓	✓
White list	✓	✗
Black list	✗	✗
Mobile Management	✓	✗
Solution for Web	Yes	No

Office 365 Notes

Whilst both products appear to do the same, there are a number of differences, these include

1. It should be noted that Archiving is provided just on a per user level. Customers who want an archive that provides a scalable, centralised, searchable solution will require a 3rd party service.
2. The selection of Anti-virus engines used by Microsoft is not published. Clearswift use Sophos and Kaspersky
3. Whilst both products use binary file type detection; Office365 has a much reduced file format set. Both products will detect attachments even if renamed
4. Office365 supports the concept of Message Quarantine, however it is a single quarantine unlike the SEG which can provide different quarantines for different policy violations with different administrator access control to each area if required
5. Both products use the concept of "fingerprinting" documents. Office365 DLP uses a method whereby the template document is used to train the system and when copies of that document are sent/received then the document type is detected. The Clearswift approach is to fingerprint the document data, and detect partial matches irrespective of whether the data is used in that templated document.
6. System logging data cannot be provided to customers (SIEM) due to the multi-tenanted nature of O365. This will impact customers who wish to gather information about data flows in/out of the business.
7. Office 365 report retention period limited to 180 days, compared to SEG 365 days.