Anti-Malware

The Clearswift SECURE Gateways provide a number of ways to eliminate the risk of malware entering or proliferating around an organization.

The primary methods of malware detection will be performed through the use of Sophos and Kaspersky Anti-Virus.

In the independent AV-Test "Protection against 0-day malware attacks, inclusive of web and e-mail threats", both Anti-Virus vendors scored perfect scores against 0-day malware attacks.

Vendor	January	February	Industry Average
SOPHOS	100%	100%	99%
KASPERSKY lab	100%	100%	99%

Whilst they seem identical, deploying both can yield a significant improvement. Internal testing for March 2017 saw that although both AV engines detected 72% of traffic simultaneously, each vendor detected some malware that the other engine missed.

These results are delivered by a number of technologies employed by most Anti-Virus vendors

- Signatures – regular updates of latest AV definitions
- Cloud Lookup – realtime checks of file signatures to see if they match any newly discovered malware
- Heuristics – AV engines inspect the files for similarities with samples of known malicious files
- Behavioural – Will run the file in an emulator briefly to try and understand what the application is doing. This is how "Sandboxes" work, but they will run the application for much longer (as much as 15 minutes to scan a file).

The Gateways also employ other features to help detect malicious object.

About Clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them 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 100% visibility of their critical information 100% of the time.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at **www.clearswift.com**

UK - International HQ
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney NSW 2060
Australia

Tel: +61 2 9424 1200
Technical Support: +61 2 9424 1200
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
Germany

Tel: +49 (0) 221 8282 9888
Technical Support: +49 (0)800 1800556
Email: info@clearswift.de

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

Tel: +81 (3)5326 3470
Technical Support: 0800 100 0006
Email: info.jp@clearswift.com

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

Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com

clearswift
RUAG Cyber Security

True File Types

The Gateways recognizes over 200 file formats by their file structure and not necessarily by name. This means that if someone renames a file "Nasty Virus.Exe" to "Safe File.txt" and if the Gateway was configured to block Executables, then it would still block the file.

Active Code Detection

The Gateways can look at HTML, PDF, Office and OpenOffice formats and see if the files contain references to active code which could be used to attack a system. These files will typically be blocked.

Structural Sanitization

An extension of the Active Code Detection is to "sanitize" the file to deliver a clean copy of the data to the intended user/recipient. This can be performed on HTML, PDF, Office and OpenOffice formats and when used in an Email Gateway can also preserve a copy of the original message.

Appended Data Detection

The deep content inspection engine looks at the file formats and verifies the format, so if someone concatenates a Text file to an image file, the Gateway can still detect this scenario and if configured can block the file being transmitted.

Message Sanitization

The SECURE Email Gateway (SEG) can be configured to perform numerous operations to reduce the chances of malware entering a company

- Attachments can be removed
- URL's can be removed
- Active script in message bodies can be removed
- HTML based messages can be stripped so that only plain text messages can be delivered

Outbreak Filters

The SEG also features Outbreak Detection which is another service feed that is provided to aid the Anti-Virus defences by detecting messages that have been found to carry malware.