



DATASHEET (CLEARSWIFT)

Anti-Malware

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

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 Avira Anti-Virus (AV) software.

In recent real-world testing conducted by AV-Test in May-June 2023, both anti-virus vendors scored perfect scores against zero-day malware attacks:

	Industry Average	May	June
 Protection against zero-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 277 samples used	99.6%	100%	100%
 Protection against zero-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 277 samples used	99.6%	100%	100%

Whilst they seem identical, deploying both can yield a significant improvement. In fact, internal testing saw that although both AV engines detected 2,554, or 72%, of malicious traffic simultaneously delivered on multiple protocols.

These results are delivered by a number of technologies employed by most AV vendors:

- Signatures – Regular updates of latest AV definitions
- Cloud Lookup – Real-time 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
- Behavioral – Runs the file in an emulator briefly to try and understand what the application is doing (this is how a Cloud Sandbox works—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 objects, including zero-days, polyglots, and APT-style files.

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, as well as inside PDFs and Office/OpenOffice file formats, to see if they contain references to active code, which could be used to attack a system by a hacker. Since the active code rarely affects the information content, it is a good idea to simply remove it. This is what structural sanitization does.

Message Sanitization

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

- Attachments can be removed
- URLs 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 defenses by detecting messages that have been found to carry malware.

FORTRATM

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.