FORTRA

DATASHEET *(Clearswift)*

Sandbox

Upgrade your existing Clearswift Secure Email Gateway (SEG) with the next-gen Cloud-Sandbox from Sophos. This network sandbox offers state of the art machine learning to provide an additional layer of security against ransomware and targeted attacks, but without any more systems to manage.

Enterprise grade protection that's deployable in minutes with seamless integration into the Email Gateway.

Defense in Depth

The use of multiple AV engines in Email Gateways is common-place, and the Clearswift SEG is no exception with the ability to use Sophos and Avira anti-virus engines in parallel. To supplement this we built our own detection capability to detect, and optionally remove active code in documents. For customers who are worried about executable content entering their organization, there is a need for Sandbox technology to fully ensure that nothing that can cause harm can enter via email.

How It Works

As messages arrive at the Gateway, they are submitted for AV scanning which will check using signatures and heuristics. Files with known malware are automatically blocked/deleted[1], but executable, or has executable content that are considered suspicious by the Sophos AV engine will be further inspected.

Firstly, the hash of the file is checked in the Sandbox to see if the file has been seen by the sandbox. If it has, then its blocked/deleted as per policy, if not the file is submitted for scanning. When the file is being detonated by the Sandbox its behaviour is carefully monitored for tell-tail signs of malicious software.

Once the file has been scanned, the Sandbox passes the results of scanning back to the Gateway where the file will be blocked, dropped or subject to further checks, such as keyword search.

PRODUCT SUMMARY

KEY FEATURES

- Inspects multiple content types using a number of methods to identify whether the file contains dangerous content using Static Analysis and Machine Learning models aid detection.
- Scans executables and scripts
    - o Windows PE executables
    - o DLL
    - o VBscript & Javascript
- Scans Documents
    - o MS Office
    - o RTF
    - o PDF
- Scans Archive files
    - o Zip, BZip, Gzip
    - o RAR, TAR, 7z
    - o LHA, LZH, Cabinet

HIGHLIGHTS

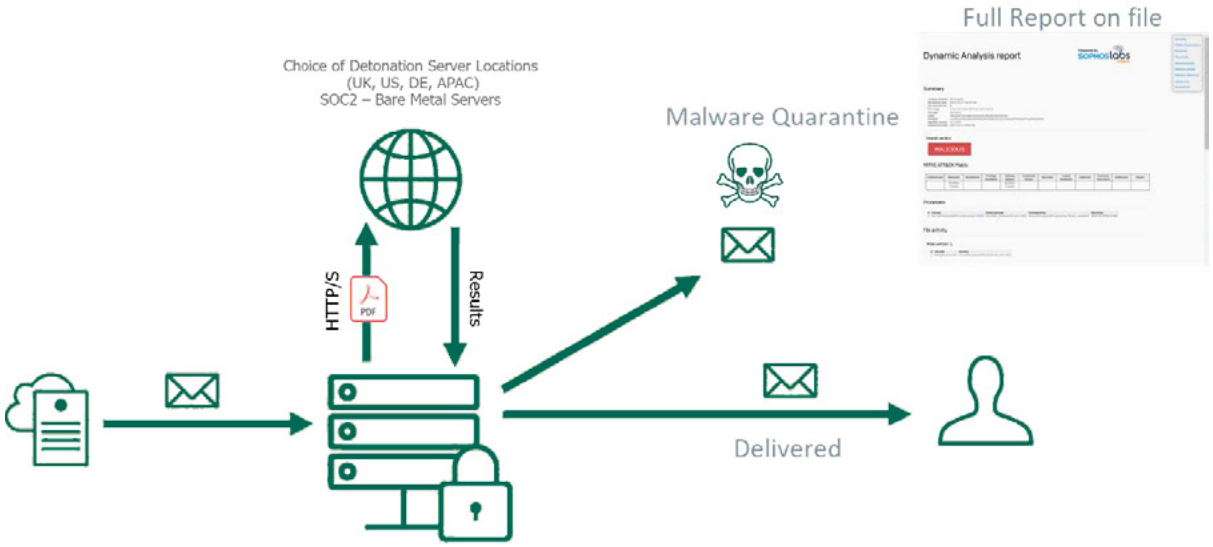
- Cloud hosted – no extra systems for customer to manage
- Secure and private detonation of content
- Support for On-premises and Hosted Gateways
- Customer choice of Sandbox location (United States, United Kingdom, Germany, Japan)
- Highly scalable AWS cloud service (SOC2)
- Low latency of scanned files, typically <5mins
- Comprehensive Analysis of file being scanned

[1] Depending on your policy

Comprehensive Reporting

If the Sandbox deems the file as dangerous it will provide a full report showing the detonation of the file for the admin team to inspect. The report will show

- File details
- File hashes
- Processes invoked
- Files written to disk
- Network Activity
- Malicious Activity
- Activity Tree
- Screenshots



FORTRA

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.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.