SOPHOS
Security made simple.

Sandstorm: Frequently asked questions

May 2017

Licensing

1. What licenses do customers need to use Sophos Sandstorm functionality?

Product and Competitive

2. Can we compare Sophos Sandstorm product with a solution as FireEye or other vendors in terms of technology and effectiveness?
3. Do we have plans for local Sandboxes as well (virtual and physical)?
4. What appliance hardware is Sophos Sandstorm compatible with?
5. Do we plan to add Sophos Sandstorm functionality to other products in the Sophos portfolio?
6. Will Sophos Sandstorm be added to Endpoint?
7. In past Gartner Magic Quadrant reports, Sophos was noted for lack of Sandbox technology. Will this assist Sophos in future reports?

Operation

8. What are the steps before a file is sent for analysis to Sophos Sandstorm?
9. Does Sophos Sandstorm scan files received in both directions inbound/outbound and refer for sandboxing?
10. Can the administrator create exclusions?
11. What file types are supported by Sophos Sandstorm?
13. How do administrators know if Sophos Sandstorm connectivity is lost/restored?
14. Which port/protocol is used to send files/hash values to the Sandstorm server?
15. Is there a local cache so there is no need to submit hashes of files inspected before?
16. What is the expected latency for Sophos Sandstorm cloud-based sandboxing?
17. Can we see a running history of how many times a suspicious file was seen and allowed or blocked?

Security and Privacy

18. How are documents kept secure in transit from Sophos products to Sophos Sandstorm?
19. Are documents encrypted when they are temporarily stored? How strong is this encryption and who has the encryption keys?
20. Are documents stored or processed by any 3rd parties?
21. In which countries or regions are files processed by Sandstorm?
22. When documents and files are executed in the sandbox, where does all the captured activity data go?
23. How long does Sophos or its affiliates keep documents?
24. Can Sophos Staff access documents or the data on them?
25. Besides documents is any other customer data sent to Sandstorm?
26. What happens if a datacenter is unavailable for processing files?

Licensing

1. What licenses do customers need to use Sophos Sandstorm functionality?

The Sandstorm license is purchased in addition to the customers' existing XG, SWA, SEA or UTM license. Details can be found in the current price list.

Please note that with both XG and UTM:

1. The Web Protection license is required to enable Sandstorm to inspect suspicious Web downloads.
2. The Email Protection license is required to enable Sandstorm to inspect suspicious emails.

Product and Competitive

2. Can we compare Sophos Sandstorm product with a solution as FireEye or other vendors in terms of technology and effectiveness?

Yes. We are using both the Sophos Labs expertise and tools alongside leading 3rd party solutions. We are very confident that our solution is as effective if not better than our competitors.

3. Do we have plans for local Sandboxes as well (virtual and physical)?

A local sandbox solution is not planned at this time.

4. What appliance hardware is Sophos Sandstorm compatible with?

- Secure Web Appliance (SWA) hardware running version 4.2 or later
- Secure Email Appliance (SEA) hardware running version 4.0 or later
- UTM hardware running version 9.4 or later
- XG hardware running version 16.05 or later

5. Do we plan to add Sophos Sandstorm functionality to other products in the Sophos portfolio?

Yes. Integration in other products is planned and will be published in the future.

6. Will Sophos Sandstorm be added to Endpoint?

Currently, there are no plans to add Sandstorm technology to Endpoint.

7. In past Gartner Magic Quadrant reports, Sophos was noted for lack of Sandbox technology. Will this assist Sophos in future reports?

Yes. The addition of sandboxing technology to our products has been welcomed by Gartner and will assist us in all future Gartner MQs.

Operation

8. What are the steps before a file is sent for analysis to Sophos Sandstorm?

Not all files are sent to the Sandstorm sandbox. There are multiple decision steps taken before a file is uploaded for analysis:

1. Anti-virus engine(s) scan files using multiple technologies to determine if there is already knowledge about the file.
2. The file is determined as known good, known bad or unknown.
3. Known bad files are blocked, known good files are released to the end-user.
4. For unknown files, depending on the file type (determined using true file type detection) Sophos anti-virus will determine if the file has any active content (e.g. Macros in Office documents or JavaScript in pdfs).
5. If there is no active content the file is considered safe and released to the end-user.
6. If active content is detected, a hash value of the file is sent to Sandstorm to check if this file has previously been analyzed.
7. If the file has previously been analyzed a result is sent back. If it is malicious, the file will be blocked. If safe, the file is released to the end-user.
8. If the file is unknown by Sandstorm, the file type is supported by Sophos Sandstorm (determined using true file type detection) and there is active content, the file will be uploaded to Sophos Sandstorm and detonated (executed in the sandbox environment) for further analysis. If the file is malicious, the file will be blocked. If safe, the file is released to the end-user.

9. Does Sophos Sandstorm scan files received in both directions inbound/outbound and refer for sandboxing?

For SWA, UTM and XG Web proxy, only downloaded files will be scanned and possibly sent to Sandstorm. For SEA, XG and UTM Email Protection both received and sent emails file attachments will be inspected by Sandstorm if suspicious.

10. Can the administrator create exclusions?

The existing AV exclusion options in XG, SWA and UTM will also apply to Sandstorm. There are no AV exclusions available in SEA.

11. What file types are supported by Sophos Sandstorm?

Sandstorm supports the file types listed below, determined by true filetype detection. If there is a specific file type you are looking for, which isn't on the list please open a ticket with support.

- PE and EXE files, including 32 or 64-bit programs, and 32 and 64-bit DLLs
- Microsoft Office Word Documents with file extensions of .doc, .docx, .docm, or .rtf
- Microsoft Office Excel Documents with file extensions of .xls, .xlsx, or .xlsm
- Microsoft Office PowerPoint documents with file extensions of .ppt, .pptx, or .pptm
- PDF documents (.pdf)

- PDF XML documents (.xpf)
- ActiveMime
- Archives (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, XZ)

12. What operating system environments does Sandstorm emulate?

Sandstorm emulates Windows environments.

13. How do administrators know if Sophos Sandstorm connectivity is lost/restored?

Connection issues are logged in the sandstorm activity log, which administrators can search. There is no connectivity status indicator or automatic alerting at this time.

14. Which port/protocol is used to send files/hash values to the Sandstorm server?

By default the product uses port 443 to communicate with the Sandstorm server. If an upstream proxy is defined, the proxy settings will be used. Please make sure that your appliance can reach sandbox.sophos.com.

15. Is there a local cache so there is no need to submit hashes of files inspected before?

Yes. The sandbox results for files that have been seen in the previous 24 hours are kept in the local cache on the appliance, reducing traffic and improving performance. In addition the sandbox servers keep a cache of hashes seen before, so files are only analyzed once.

16. What is the expected latency for Sophos Sandstorm cloud-based sandboxing?

For files that are present in the cache or have been previously analyzed this will be seconds. Files, which will need to be uploaded and fully analyzed, will take up to 20 minutes with an average of 5 minutes.

17. Can we see a running history of how many times a suspicious file was seen and allowed or blocked?

There is a counter of files submitted and reporting on the number deemed malicious or clean. The malicious files report also shows if we needed to submit the file or if Sophos Labs had previously identified the threat.

Security and Privacy

18. How are documents kept secure in transit from Sophos products to Sophos Sandstorm?

Samples are submitted to Sophos servers running on Amazon hosted cloud servers over standard HTTPS protocol. The files are asymmetrically encrypted by the servers before being written to Amazon hosted storage, transferred to Sophos hosts infrastructure where the decryption key is held. At this point they are decrypted for processing.

19. Are documents encrypted when they are temporarily stored? How strong is this encryption and who has the encryption keys?

When samples are not being processed, such as when in transit or in temporary storage, they are encrypted with industry standard asymmetric encryption with the private key held on physical Sophos infrastructure.

20. Are documents stored or processed by any 3rd parties?

The Sophos Sandstorm sandbox solution uses a combination of Sophos and a select 3rd party for sample processing. For security reasons, Sophos do not disclose information about the technology partners. All 3rd party technology partners used by Sophos are vetted and contractually obliged to apply the same security and privacy polices used by Sophos in the handling of sandbox samples. For 3rd parties used for temporary cloud storage, samples are stored encrypted with the private key held by Sophos.

21. In which countries or regions are files processed by Sandstorm?

This depends on the features or location of your Sophos product. Currently (April 2017):

Sandstorm data centers are located in the European Union and in the USA.

For Sophos XG Firewall and Sophos Web Appliance the data center location is configurable. The administrator of the device can specify that either the European Union data center or the USA data center processes suspicious files. Files are sent SSL-encrypted to Sandstorm.

If the administrator chooses automatic selection, the device uses Latency Based Routing (LBR) (see point 3 below) to direct suspicious customer files to the appropriate data center.

For Sophos UTM and Sophos Email Appliance:

1. If the Sophos Appliance is located in Europe, SSL-encrypted files are sent to the European Union Sandstorm data center (see point 3).
2. If the Sophos Appliance is located in the USA, SSL-encrypted files are sent to the USA Sandstorm data center. For all other appliance locations, files are sent to the Sandstorm data center that is closest to the appliance location (see point 3).
3. Sophos uses Latency Based Routing (LBR) to direct suspicious customer files to the appropriate data center. This relies on the latency between the customer DNS resolver and Amazon name servers. In order to ensure suspicious files are sent to the correct data center it is important to configure your Sophos appliance to use an appropriate DNS server. Sophos appliances configured to use a Europe DNS server sends files to the European Union Sandstorm data center. Sophos appliances configured to use a US DNS server direct files to the to the US Sandstorm data center. Appliances configured with DNS servers in other locations direct files to the LBR-derived closest location of the two data centers.

22. When documents and files are executed in the sandbox, where does all the captured activity data go?

The file copy is detonated in the safe confines of Sandstorm and monitored for malicious behavior. All processing is done in RAM. All suspicious files are cleared from memory after analysis is complete.

The only exception is where malicious files are discovered. In this case, these files are retained and are further analyzed. This analysis is then used to update other protection technologies. A decision to allow or block the file will be sent to the security solution once the analysis is complete.

If the file copy is benign, the original file will be released to the end-user. Malicious files attached to emails will remain in quarantine until further action is taken by an administrator. Malicious files intercepted by web filtering will be deleted immediately.

Sophos Sandstorm also stores file hash values and results for faster overall responses. Files are only uploaded once. No filename or other meta data is stored for this purpose.

23. How long does Sophos or its affiliates keep documents?

If no malicious activity is detected, the encrypted Sandbox sample file and analysis report are retained for 30 days. If the file is malicious, the Sandbox sample file and analysis report are stored for an unlimited amount of time in order to support global protection efforts.

24. Can Sophos Staff access documents or the data on them?

No, general Sophos staff has no access to sandbox samples. In some rare and specific cases, sandbox service engineers and or security researchers assigned to the sandbox services may require access to a sample in order to trouble shoot or enhance the service. This access is done within a secure, isolated area. No samples are copied or removed from this isolated area.

25. Besides documents is any other customer data sent to Sandstorm?

For authentication purposes the device serial number is sent to Sandstorm. In addition, for Web downloads, the URL of the download is sent, excluding possible parameters which might contain private information.

26. What happens if a datacenter is unavailable for processing files?

If the EU or US datacenter is unavailable there is no failover to the alternative data center location. For example, if the Sophos Appliance is located in Europe and the EU Sandstorm data center is unavailable, the Sophos Appliance will not send files to the US data center.