SOPHOS
Security made simple.

Sandstorm: FAQs

Mai 2016

Lizenzen

1. Welche Lizenzen benötigen die Kunden, um die Sophos Sandstorm-Funktionalität nutzen zu können?

Produkt und Wettbewerbsvorteil

2. Ist das Sophos Sandstorm-Produkt mit einer Lösung wie FireEye oder anderen Konkurrenzprodukten im Hinblick auf Technologie und Effizienz zu vergleichen?
3. Sind auch lokale Sandbox-Lösungen geplant (virtuell und physisch)?
4. Mit welcher Appliance-Hardware ist Sophos Sandstorm kompatibel?
5. Ist geplant, die Sophos Sandstorm-Funktionalität in andere Produkte des Sophos-Portfolios zu integrieren?
6. Wird Sophos Sandstorm auch in Endpoint integriert?
7. In den letzten Gartner Magic Quadrant Reports wurde bemängelt, dass Sophos keine Sandbox-Technologie hat. Wird sich das in den nächsten Reports ändern?

Betrieb

8. Welche Schritte sind der Übermittlung einer Datei zu Sophos Sandstorm zwecks Analyse vorgelagert?
9. Scannt Sophos Sandstorm ein- und ausgehende Dateien und schickt sie zum Sandboxing?
10. Kann der Administrator Ausschlüsse festlegen?
11. Welche Dateitypen werden von Sophos Sandstorm unterstützt?
13. Wie erfahren die Administratoren, ob die Sophos Sandstorm-Verbindung unterbrochen/wiederhergestellt wurde?
14. Welcher Port/welches Protokoll wird verwendet, um Dateien/Hash-Werte zum Sandstorm-Server zu schicken?
15. Gibt es einen lokalen Cache, so dass keine Hashes von bereits geprüften Dateien übermittelt werden müssen?
16. Wie hoch ist die voraussichtliche Latenz beim cloudbasierten Sophos Sandstorm Sandboxing?
17. Gibt es einen Verlauf, aus dem ersichtlich ist, wie oft eine verdächtige Datei erkannt und erlaubt oder blockiert wurde?

Sicherheit und Datenschutz

18. Wie wird die Sicherheit der Dokumente während der Übertragung von Sophos-Produkten an Sophos Sandstorm gewährleistet?
19. Sind die Dokumente verschlüsselt, wenn sie vorübergehend gespeichert werden? Wie stark ist diese Verschlüsselung und wer besitzt die Verschlüsselungsschlüssel?
20. Werden Dokumente von Dritten gespeichert oder verarbeitet?
21. In welchen Ländern oder Regionen werden Dateien von Sandstorm verarbeitet?

22. Was geschieht mit den erfassten Aktivitätsdaten, wenn Dokumente und Dateien in der Sandbox ausgeführt werden?
23. Wie lange bewahren Sophos oder dessen Partner Dokumente auf?
24. Haben die Mitarbeiter von Sophos Zugriff auf Dokumente oder die darin enthaltenen Daten?
25. Werden neben Dokumenten auch andere Kundendaten an Sandstorm geschickt?

Lizenzen

1. Welche Lizenzen benötigen die Kunden, um die Sophos Sandstorm-Funktionalität nutzen zu können?

Die Sandstorm-Lizenz wird zusätzlich zur vorhandenen SWA-, SEA- oder UTM-Lizenz des Kunden erworben. Nähere Informationen entnehmen Sie bitte der aktuellen Preisliste.

Produkt und Wettbewerbsvorteil

2. Ist das Sophos Sandstorm-Produkt mit einer Lösung wie FireEye oder anderen Konkurrenzprodukten im Hinblick auf Technologie und Effizienz zu vergleichen?

Ja. Wir greifen zusätzlich zum Know-how und zu den Tools der Sophos Labs auf führende Lösungen von Drittanbietern zurück. Wir sind überzeugt, dass unsere Lösung genauso effizient, wenn nicht sogar besser als die unserer Mitbewerber ist.

3. Sind auch lokale Sandbox-Lösungen geplant (virtuell und physisch)?

Eine lokale Sandbox-Lösung ist aktuell nicht geplant.

4. Mit welcher Appliance-Hardware ist Sophos Sandstorm kompatibel?

- Secure Web Appliance (SWA)-Hardware Version 4.2 oder höher
- Secure Email Appliance (SEA)-Hardware Version 4.0 oder höher
- UTM-Hardware Version 9.4 oder höher

5. Ist geplant, die Sophos Sandstorm-Funktionalität in andere Produkte des Sophos-Portfolios zu integrieren?

Ja. SWA, SEA und UTM sind die ersten Produkte, die Sophos Sandstorm unterstützen. Wir werden Sophos Sandstorm in einem der nächsten Releases auch in die XG Firewall integrieren. Zurzeit ist die Sophos Sandstorm-Integration für SFOS 17 der XG Firewall geplant. Die Integration in andere Produkte ist geplant; Informationen dazu werden zu einem späteren Zeitpunkt bekanntgegeben.

6. Wird Sophos Sandstorm auch in Endpoint integriert?

Es ist geplant, die Sandstorm-Technologie in zukünftige Releases von Sophos Central und Endpoint Security zu integrieren. Wir werden zu einem späteren Zeitpunkt über neue Produkte informieren.

7. In den letzten Gartner Magic Quadrant Reports wurde bemängelt, dass Sophos keine Sandbox-Technologie hat. Wird sich das in den nächsten Reports ändern?

Ja. Dass in unsere Produkte jetzt die Sandbox-Technologie integriert ist, wurde von Gartner begrüßt und wird sich positiv in allen künftigen Gartner MQs niederschlagen.

Betrieb

8. Welche Schritte sind der Übermittlung einer Datei zu Sophos Sandstorm zwecks Analyse vorgelagert?

Nicht alle Dateien werden zur Sandstorm-Sandbox geschickt. Bevor eine Datei zur Analyse übermittelt wird, finden mehrere Entscheidungsschritte statt:

1. Anti-Virus-Engines scannen die Dateien mithilfe verschiedener Technologien, um festzustellen, ob die Datei bereits bekannt ist.
2. Die Datei wird in eine der Kategorien „als unschädlich bekannt“, „als schädlich bekannt“ oder „unbekannt“ eingestuft.
3. Als schädlich bekannte Dateien werden blockiert, als unschädlich bekannte Dateien werden für den Endbenutzer freigegeben.
4. Bei unbekannten Dateien prüft Sophos Anti-Virus je nach Dateityp (der mithilfe der True File Type-Erkennung ermittelt wird), ob die Datei aktive Inhalte aufweist (z. B. Makros in Office-Dokumenten oder JavaScript in PDFs).
5. Weist die Datei keine aktiven Inhalte auf, wird die Datei als sicher betrachtet und für den Endbenutzer freigegeben.
6. Wird aktiver Inhalt erkannt, wird ein Hash-Wert der Datei an Sandstorm geschickt, damit überprüft wird, ob die Datei vorher schon einmal analysiert wurde.
7. Wurde die Datei bereits analysiert, wird ein Ergebnis zurückgeschickt. Ist die Datei schädlich, wird sie blockiert. Ist sie sicher, wird sie für den Endbenutzer freigegeben.
8. Wenn Sandstorm die Datei nicht kennt, der Dateityp von Sophos Sandstorm (der mithilfe der True File Type-Erkennung ermittelt wird) unterstützt wird und die Datei aktive Inhalte aufweist, wird die Datei an Sophos Sandstorm übertragen und in der sicheren Sandbox-Umgebung zur weiteren Analyse ausgeführt. Ist die Datei schädlich, wird sie blockiert. Ist sie sicher, wird sie für den Endbenutzer freigegeben.

9. Scannt Sophos Sandstorm ein- und ausgehende Dateien und schickt sie zum Sandboxing?

Bei SWA und dem UTM Web-Proxy werden nur heruntergeladene Dateien gescannt und gegebenenfalls an Sandstorm geschickt. Bei SEA und UTM Email Protection werden sowohl empfangene als auch gesendete E-Mail-Anhänge von Sandstorm geprüft, wenn diese verdächtig sind.

10. Kann der Administrator Ausschlüsse festlegen?

Ja. Die in den Produkten vorhandenen AV-Ausschlussoptionen gelten auch für Sandstorm.

11. Welche Dateitypen werden von Sophos Sandstorm unterstützt?

Sandstorm unterstützt die nachfolgend genannten Dateitypen, die mithilfe der True File Type-Erkennung ermittelt werden. Falls Sie in der Liste einen bestimmten Dateityp vermissen, öffnen Sie bitte ein Support-Ticket.

- PE- und EXE-Dateien, einschließlich 32- oder 64-Bit-Programme, und 32- und 64-Bit-DLLs
- DOS-Executables (.exe)
- COM-Executables (.com)
- Microsoft Batch-Scripts (außer in Fällen, in denen die Dateien gestreamt wurden)
- Microsoft-Installationsdateien (.msi)
- Microsoft Office Word-Dokumente mit der Dateiendung .doc, .docx, .docm oder .rtf
- Microsoft Office Excel-Dokumente mit der Dateiendung .xls, .xlsx oder .xlsm
- Microsoft Office PowerPoint-Dokumente mit der Dateiendung .ppt, .pptx oder .pptm
- Hangul Office-Dokumente (.hwp)
- PDF-Dokumente (.pdf)
- PDF XML-Dokumente (.xpf)
- Microsoft-Hilfedateien (.chm)
- Android-Apps (.apk)
- Java JARs und Klassendateien (.jar, .class)
- WordPerfect (.wpd)
- Adobe Flash (.swf), in FWS-, CWS-, ZWS-Varianten
- ActiveMime
- Archive (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, XZ)

12. Welche Betriebssystem-Umgebungen emuliert Sandstorm?

Sandstorm emuliert Windows-, Mac OSX- und Android-Sandboxumgebungen.

13. Wie erfahren die Administratoren, ob die Sophos Sandstorm-Verbindung unterbrochen/wiederhergestellt wurde?

Verbindungsprobleme werden im Sandstorm-Aktivitätsprotokoll erfasst, in dem die Administratoren eine Suche vornehmen können. Es gibt im Moment noch keine Verbindungsstatus-Anzeige oder automatische Benachrichtigung.

14. Welcher Port/welches Protokoll wird verwendet, um Dateien/Hash-Werte zum Sandstorm-Server zu schicken?

Standardmäßig verwendet das Produkt für die Kommunikation mit dem Sandstorm-Server Port 443. Ist ein Upstream-Proxy festgelegt, werden die Proxy-Einstellungen verwendet. Stellen Sie sicher, dass Ihre Appliance sandbox.sophos.com erreichen kann.

15. Gibt es einen lokalen Cache, so dass keine Hashes von bereits geprüften Dateien übermittelt werden müssen?

Ja. Die Sandbox-Ergebnisse für Dateien, die in den letzten 24 Stunden geprüft wurden, verbleiben im lokalen Cache auf der Appliance, was den Datenverkehr verringert und die Leistung verbessert. Darüber hinaus verfügen die Sandbox-Server über einen Cache mit bereits bekannten Hashes, so dass Dateien nur einmal analysiert werden müssen.

16. Wie hoch ist die voraussichtliche Latenz beim cloudbasierten Sophos Sandstorm Sandboxing?

Bei Dateien im Cache oder solchen, die bereits analysiert wurden, sind es Sekunden. Bei Dateien, die übertragen und vollständig analysiert werden müssen, dauert es bis zu 20 Minuten, der Durchschnitt liegt bei 5 Minuten.

17. Gibt es einen Verlauf, aus dem ersichtlich ist, wie oft eine verdächtige Datei erkannt und erlaubt oder blockiert wurde?

Es gibt einen Zähler für übermittelte Dateien und Berichte über die Anzahl der als schädlich oder sicher eingestuften Dateien. Der Bericht über schädliche Dateien gibt auch Auskunft darüber, ob wir die Datei weiterleiten mussten oder ob die Bedrohung bereits von den Sophos-Labs erkannt wurde.

Sicherheit und Datenschutz

18. Wie wird die Sicherheit der Dokumente während der Übertragung von Sophos-Produkten an Sophos Sandstorm gewährleistet?

Die Samples werden über das Standard-HTTPS-Protokoll an die Sophos-Server übertragen, die auf von Amazon gehosteten Cloud-Servern ausgeführt werden. Die Dateien werden von den Servern asymmetrisch verschlüsselt, bevor sie in den von Amazon gehosteten Speicher geschrieben und zu der von Sophos gehosteten Infrastruktur übertragen werden, wo der Entschlüsselungsschlüssel gespeichert ist. An dieser Stelle werden sie für die Verarbeitung entschlüsselt.

19. Sind die Dokumente verschlüsselt, wenn sie vorübergehend gespeichert werden? Wie stark ist diese Verschlüsselung und wer besitzt die Verschlüsselungsschlüssel?

Wenn sich Samples nicht in Verarbeitung befinden, z. B. während der Übertragung oder im vorübergehenden Speicher, werden sie mit der branchenüblichen asymmetrischen Verschlüsselung verschlüsselt, wobei der private Schlüssel in der physischen Infrastruktur von Sophos gespeichert ist.

20. Werden Dokumente von Dritten gespeichert oder verarbeitet?

Die Sophos Sandstorm Sandbox-Lösung greift für die Verarbeitung der Samples auf Sophos-eigene Ressourcen und auf einen ausgewählten externen Technologiepartner zurück. Aus Sicherheitsgründen gibt Sophos keine Informationen über die Technologiepartner bekannt. Alle externen Technologiepartner, mit denen Sophos zusammenarbeitet, wurden überprüft und vertraglich verpflichtet, beim Umgang mit den Sandbox-Samples dieselben Sicherheits- und Datenschutzrichtlinien zu beachten wie Sophos. Erfolgt die Nutzung externer Technologiepartner für die temporäre Cloud-Speicherung, werden die Samples mit dem von Sophos gespeicherten privaten Schlüssel verschlüsselt gespeichert.

21. In welchen Ländern oder Regionen werden Dateien von Sandstorm verarbeitet?

Dies hängt vom SWA-, SEA- oder UTM-Standort ab. Aktuell (Mai 2016):

1. Die Sandstorm-Datencenter befinden sich in den Niederlanden und den USA. Wenn sich die Sophos Appliance in Europa befindet, werden die SSL-verschlüsselten Dateien zum Sandstorm-Datencenter in den Niederlanden geschickt (siehe Punkt 3).
2. Befindet sich die Sophos Appliance in den USA, werden die SSL-verschlüsselten Dateien zum Sandstorm-Datencenter in den USA geschickt. Bei allen anderen Appliance-Standorten werden die Dateien zu dem Sandstorm-Datencenter geschickt, das sich am nächsten befindet (siehe Punkt 3).
3. Sophos leitet verdächtige Kundendateien mit Latency Based Routing (LBR) an das jeweilige Datencenter weiter. Das Routing basiert dabei auf der Latenz zwischen dem DNS-Resolver des Kunden und den Amazon Name-Servern. Damit verdächtige Dateien an das richtige Datencenter geschickt werden, muss in Ihrer Sophos Appliance ein entsprechender DNS-Server konfiguriert sein. Sophos Appliances, die so konfiguriert sind, dass ein DNS-Server in Europa genutzt wird, schicken Dateien an das Sandstorm-Datencenter in Europa. Sophos Appliances, die so konfiguriert sind, dass ein DNS-Server in den USA genutzt wird, leiten Dateien an das Sandstorm-Datencenter in den USA weiter. Appliances, auf denen DNS-Server an anderen Standorten konfiguriert sind, leiten die Dateien an den vom LBR abgeleiteten nächsten Datencenter-Standort weiter.

22. Was geschieht mit den erfassten Aktivitätsdaten, wenn Dokumente und Dateien in der Sandbox ausgeführt werden?

Die Dateikopie wird in der sicheren Sandbox von Sandstorm ausgeführt und auf schädliche Verhaltensweisen überwacht. Die gesamte Verarbeitung erfolgt im RAM. Alle verdächtigen Dateien werden nach Abschluss der Analyse aus dem Speicher gelöscht, es sei denn, es wurden schädliche Dateien erkannt. In diesem Fall bleiben die Dateien im Speicher und werden weiter analysiert. Anhand der Ergebnisse dieser Analyse werden dann die anderen Schutztechnologien aktualisiert. Nach Abschluss der Analyse wird die Entscheidung an die Sicherheitslösung übermittelt, ob die Datei zugelassen oder blockiert werden soll.

Ist die Dateikopie harmlos, wird die Ursprungsdatei für den Endbenutzer freigegeben. Schädliche Dateien, die an E-Mails angehängt waren, bleiben in Quarantäne, bis der Administrator weitere Maßnahmen ergreift. Schädliche Dateien, die vom Webfilter abgefangen wurden, werden sofort gelöscht.

Sophos Sandstorm speichert auch die Hash-Werte der Datei und die Ergebnisse, um den Vorgang insgesamt zu beschleunigen. Dateien werden nur einmal übertragen. Für diesen Zweck werden keine Dateinamen oder andere Metadaten gespeichert.

23. Wie lange bewahren Sophos oder dessen Partner Dokumente auf?

Wenn keine schädliche Aktivität festgestellt wurde, wird die Datei nicht gespeichert. Ist die Datei schädlich, wird sie für unbegrenzte Zeit gespeichert, um die weltweiten Sicherheitsbemühungen zu unterstützen.

24. Haben die Mitarbeiter von Sophos Zugriff auf Dokumente oder die darin enthaltenen Daten?

Nein, in der Regel haben die Mitarbeiter von Sophos keinen Zugriff auf die Sandbox-Samples. In bestimmten seltenen Fällen kann es sein, dass die Sandbox-Servicetechniker und/oder Sicherheitsexperten, die mit den Sandbox-Services betraut sind, Zugriff auf ein Sample erhalten, um Probleme zu beheben oder den Service zu erweitern. Dieser Zugriff erfolgt in einem sicheren, isolierten Bereich. In diesem isolierten Bereich werden keine Samples kopiert oder entfernt.

25. Werden neben Dokumenten auch andere Kundendaten an Sandstorm geschickt?

Für Erkennungszwecke wird die Seriennummer des Geräts an Sandstorm übermittelt. Darüber hinaus wird bei Web-Downloads die URL des Downloads übermittelt, aber ohne etwaige Parameter, die private Informationen enthalten könnten.

Sophos GmbH
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Deutschland

Amtsgericht Wiesbaden HRB 25915,
Ust.-ID Nr. DE189 689 369

Tel.: +49 (0)611 5858-0
E-Mail: info@sophos.de