SOPHOS
Security made simple.

Sophos Sandstorm und Datenschutz

Sophos Sandstorm ist eine leistungsstarke cloudbasierte Next-Generation Sandbox, die evasive Zero-Day-Malware erkennt, blockiert und Reports über diese generiert. Eine Sandbox ist eine isolierte Umgebung. In ihr können verdächtige Programme gefahrlos ausgeführt werden, die sich im Anhang von E-Mails befinden oder von Websites heruntergeladen werden, um festzustellen, ob sie Malware enthalten.

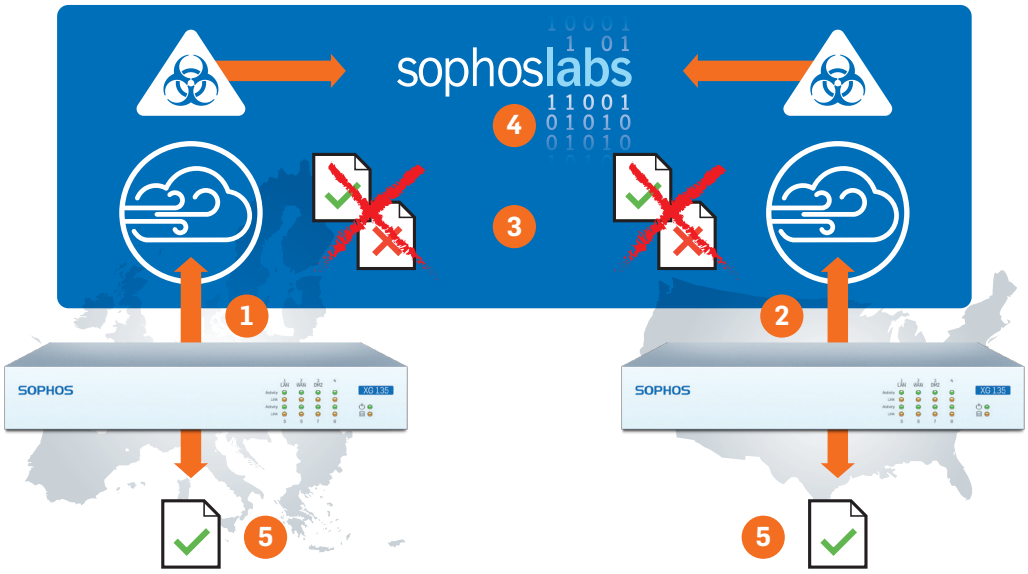
Sandstorm wird optional als Ergänzung zu den Sophos UTM, Web Appliance und Email Appliance Sicherheitslösungen angeboten.

Sofern aktiviert, werden im Rahmen der Sandstorm-Analyse Kopien verdächtiger Dateien an ein Sandstorm-Datencenter geschickt. In diesem Dokument ist erklärt, wie Dateien von Ihrer Sophos Appliance und Sandstorm analysiert werden.

Sophos Appliance-Analyse:

1. Enthält eine Datei bekannte Malware, wird sie sofort auf der Sophos Appliance blockiert. Es werden keine Dateien an Sandstorm geschickt.
2. Ist die Datei in anderer Form verdächtig und wird sie zum ersten Mal erkannt, wird eine Kopie der Datei zur weiteren Analyse an Sandstorm geschickt. Die ursprüngliche Datei bleibt auf der Appliance in Quarantäne.

Sophos Sandstorm-Analyse:



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*.
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*.
3. Die Dateikopie wird in der sicheren Sandbox ausgeführt und auf schädliche Verhaltensweisen überwacht. Die gesamte Verarbeitung erfolgt im RAM. Alle verdächtigen Dateien werden nach Abschluss der Analyse aus dem Speicher gelöscht,
4. 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.
5. 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 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.

Weitere Informationen über die SophosLabs Richtlinien zur Informationssicherheit finden Sie hier.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

16-07-01 DE (NP)

SOPHOS