

# Sophos Sandstorm

## Einfache und leistungsstarke Bedrohungsabwehr der nächsten Generation

Sophos ist in der IT-Sicherheitsbranche Vorreiter bei der Bekämpfung von Malware mit hocheffektiven Technologien wie JavaScript-Emulation in Echtzeit und Verhaltensanalysen. Herkömmlicher Malware-Schutz ist als erste Verteidigungslinie nach wie vor wichtig. Unternehmen benötigen jedoch weitere Tools, um gezielte Malware zuverlässig abwehren zu können.



Sophos Sandstorm ist unsere Lösung zur Abwehr von Advanced Persistent Threats (APT) und Zero-Day-Malware und kann als ergänzendes Feature mit Sophos-Sicherheitsprodukten verwendet werden. Durch Einsatz leistungsstarker cloudbasierter Next-Generation-Sandbox-Technologie ermöglicht Sophos Sandstorm eine schnelle und zuverlässige Erkennung, Blockierung und Reaktion auf evasive Malware, die andere Lösungen übersehen.

### Highlights

- ▶ Nahtlose Integration in Ihre Sophos-Sicherheitslösung
- ▶ Innerhalb von Minuten einsatzbereit
- ▶ Schützt vor APTs, unbekannter Malware und gezielten Angriffen
- ▶ Liefert Bedrohungsdaten, die eine schnelle Reaktion ermöglichen
- ▶ Breite Plattformabdeckung
- ▶ Detaillierte, ereignisorientierte Reports

### Erweiterter Schutz vor gezielten Angriffen

Halten Sie unbekannte datenstehlende Malware aus Ihrem Netzwerk fern. Mit unserer leistungsstarken cloudbasierten Next-Generation-Sandbox-Technologie können Sie APTs und Zero-Day-Bedrohungen schnell und zuverlässig erkennen, blockieren und auf sie reagieren.

### Einfache Implementierung

Sophos Sandstorm ist komplett in Ihre Sophos-Sicherheitslösung integriert. Sie müssen lediglich Ihre Subscription aktualisieren, die Sandstorm-Richtlinie anwenden und schon sind Sie vor gezielten Angriffen geschützt. Der ganze Vorgang dauert nur wenige Minuten.

### Blockiert evasive Malware, die andere übersehen

Mit Sophos Sandstorm erkennen Sie auch unbekannte Bedrohungen, die speziell entwickelt wurden, um Sandbox-Appliances der ersten Generation zu umgehen. Mit unserem systemübergreifenden Emulationsansatz erhalten Sie einen detaillierten Einblick in das Verhalten unbekannter Malware und die Erkennung von Malware-Angriffen, die andere einfach übersehen.

### Forensik-Reports

Reagieren Sie mit einer einfachen, ereignisorientierten Analyse von Sicherheitsverletzungen schneller auf hochentwickelte Bedrohungen. Wir liefern Ihnen priorisierte APT-Daten, die auf einer Korrelation von Beweisen basieren. Dieser Ansatz reduziert nicht nur Störungen, sondern spart Ihnen auch Zeit.

### Umfassende Analyse

Decken Sie potenziell schädliche Verhaltensweisen auf all Ihren Endbenutzer-Geräten und in allen kritischen Infrastrukturen auf. Hierzu zählen Ihre Betriebssysteme (Windows, Mac OS X und Android), physische und virtuelle Hosts, Dienste, Netzwerkinfrastrukturen sowie Web-, E-Mail-, Datei- und mobile Anwendungen. Bedrohungen können in der Sandstorm-Cloud sicher ausgeführt werden, sodass keine Gefährdung durch gefährliche Malware für Ihre Rechenzentren besteht.

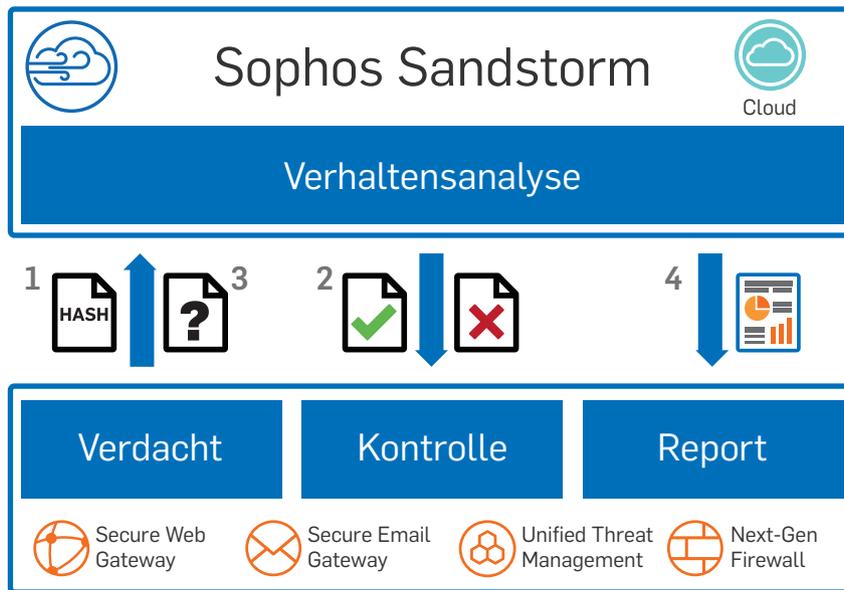
### Blitzschnelle Performance

Ihre Sophos-Sicherheitslösung nimmt eine präzise Vorfilterung Ihres Datenverkehrs vor, sodass nur verdächtige Dateien an Sandstorm gesendet werden. Auf diese Weise stellen wir sicher, dass die Latenz und Beeinträchtigung der Endbenutzer so gering wie möglich ist.

## Features von Sophos Sandstorm

- › Dynamische Malware-Verhaltensanalyse führt Dateien in realen Umgebungen aus
- › Komplette Integration in das Dashboard Ihrer Sophos-Sicherheitslösung
- › Prüft über 40 Dateitypen, u. a.:
  - PE (ausführbare 32- oder 64-Bit-Programme und DLLs)
  - Microsoft-Office-Dokumente (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .docm, .xlsm, .pptm, .rtf)
  - PDF, HWP, XPF, CHM, JAR, APK-Archive (ZIP, BZIP, GZIP, RAR, TAR, LHA LZH, XZ)
- › Detaillierte Reports zu Schaddateien und Möglichkeit zur Dashboard-Dateifreigabe
  - Durchschnittliche Analysedauer weniger als 120 Sekunden
  - Flexible Richtlinienoptionen für Dateigröße und -typ, Ausnahmen und Analyseaktionen
  - Prüft den gesamten Datenverkehr zu und von der Sandbox-Umgebung auf bekannten C&C-Traffic
  - Schützt eine Vielzahl von Umgebungen, u. a. Windows, Mac und Android
  - Unterstützt Einmal-Download-Links

## Funktionsweise



1. Die Sophos-Sicherheitslösung testet die potenzielle Bedrohung unter Anwendung aller gewöhnlichen Sicherheitsüberprüfungen (z. B. Anti-Malware-Signaturen, gefährliche URLs usw.) Wird die verdächtige Datei nicht als Bedrohung erkannt, sendet die Sophos-Sicherheitslösung den Dateihash an Sophos Sandstorm, um zu ermitteln, ob die Datei bereits zuvor analysiert wurde.
2. Wenn die Datei bereits analysiert wurde, übermittelt Sophos Sandstorm die Bedrohungsdaten an die Sophos-Sicherheitslösung. Hier wird die Datei entweder an das Benutzergerät zugestellt oder blockiert – je nachdem, welche Informationen von Sophos Sandstorm übermittelt wurden.
3. Wenn der Hash noch komplett unbekannt ist, wird eine Kopie der verdächtigen Datei an Sophos Sandstorm gesendet. Hier wird die Datei ausgeführt und ihr Verhalten wird überwacht. Sobald die Datei vollständig analysiert wurde, leitet Sophos Sandstorm die Bedrohungsdaten an die Sophos-Sicherheitslösung weiter. Wieder wird die Datei entweder an das Benutzergerät zugestellt oder blockiert – je nachdem, welche Informationen von Sophos Sandstorm übermittelt wurden.
4. Die Sophos-Sicherheitslösung erstellt anhand der von Sophos Sandstorm übermittelten Detailinformationen Forensik-Reports zu jedem Bedrohungsereignis.

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter  
[www.sophos.de/sandstorm](http://www.sophos.de/sandstorm)

Sales DACH (Deutschland, Österreich, Schweiz)  
Tel.: +49 611 5858 0 | +49 721 255 16 0  
E-Mail: [sales@sophos.de](mailto:sales@sophos.de)

Oxford, GB | Boston, USA  
© Copyright 2015. Sophos Ltd. Alle Rechte vorbehalten.  
Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB  
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

2015.11.13 DS-DE (GH)

**SOPHOS**