SOPHOS
Security made simple.

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 moderne Ransomware und gezielte Malware zuverlässig abwehren zu können.

Hier hilft unsere Sicherheitslösung Sophos Sandstorm: Sie kann als Ergänzung zu bestehenden Sophos-Security-Produkten genutzt werden und wehrt Ransomware und Advanced Persistent Threats (APTs) zuverlässig ab. 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 Ransomware-APTs, unbekannter Malware und gezielten Bedrohungen
- Liefert Bedrohungsdaten, die eine schnelle Reaktion ermöglichen
- Detaillierte, ereignisorientierte Reports

Erweiterter Schutz vor gezielten Angriffen

Halten Sie Ransomware und 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 is 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

Sophos Sandstorm erkennt Ransomware und unbekannte Bedrohungen, die speziell dafür entwickelt wurden, Sandbox-Appliances der ersten Generation zu täuschen. 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.

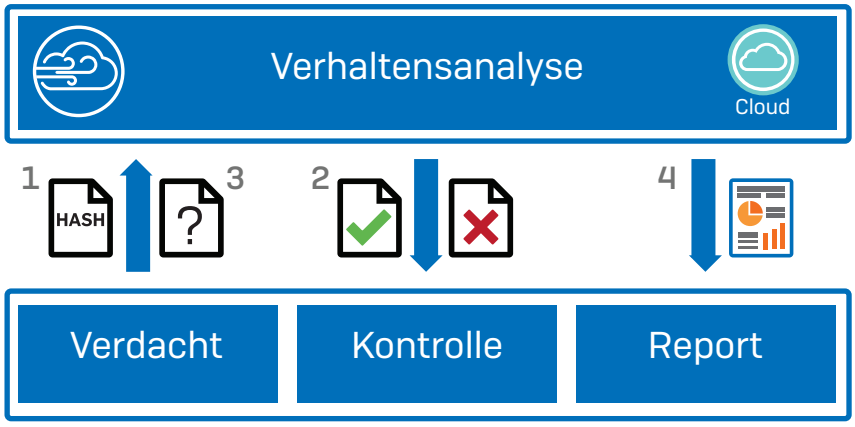
Blitzschnelle Performance

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

- Komplette Integration in das Dashboard Ihrer Sophos-Sicherheitslösung
- Überprüft ausführbare Dateien und Dokumente mit ausführbaren Inhalten
  - Ausführbare Windows-Dateien (u. a. .exe, .com und .dll)
  - Word-Dokumente (u. a. .doc, .docx, docm und .rtf)
  - PDF-Dokumente
  - Archive, die beliebige der oben aufgeführten Dateitypen (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) enthalten
  - Unterstützt mehr als 20 Dateitypen
- Dynamische Malware-Verhaltensanalyse führt Dateien in realen Umgebungen aus
- Detaillierte Reports zu Schaddateien und Möglichkeit zur Dashboard-Dateifreigabe
  - Durchschnittliche Analysedauer weniger als 120 Sekunden
  - Flexible Benutzer- und Gruppenrichtlinienoptionen für Dateityp, Ausnahmen und Maßnahmen bei der Analyse
  - Unterstützt Einmal-Download-Links

Funktionsweise



1. Die Sophos-Sicherheitslösung scannt Dateien unter Anwendung aller gewöhnlichen Sicherheitsüberprüfungen (z. B. Anti-Malware-Signaturen, gefährliche URLs usw.). Wenn die Datei ausführbar ist oder ausführbare Elemente enthält und nicht von einer sicheren Website heruntergeladen wird, wird die Datei als verdächtig gehandhabt. Die Sophos-Sicherheitslösung sendet den verdächtigen 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

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

SOPHOS

2016,11 DS-DE (SM)