SOPHOS

Cybersecurity made simple.

Sophos Sandstorm

Next-Gen-Schutz vor komplexen Bedrohungen leicht gemacht

Sophos Sandstorm bietet Ihrem Unternehmen mit Next-Gen-Cloud-Sandbox-Technologie zusätzlichen Schutz vor Ransomware und gezielten Angriffen.

Sophos Sandstorm nutzt als einzige Netzwerk-Sandbox Deep Learning-Analysen zur effektiveren Erkennung und lässt sich nahtlos mit der Sophos XG Firewall, Sophos UTM, Sophos Web Appliance, Sophos Email Appliance und Sophos Email in Sophos Central integrieren. Es ist keine zusätzliche Hardware erforderlich.

Highlights

- Nahtlose Integration in Ihre Sophos-Sicherheitslösung
- Innerhalb von Minuten einsatzbereit
- Schutz vor Ransomware und APTs, unbekannter Malware, PUAs und gezielten Angriffen
- Liefert Bedrohungsdaten, die eine schnelle Reaktion ermöglichen
- Deep Learning-Analyse
- Detaillierte, ereignisorientierte Reports

Erweiterter Schutz vor gezielten Angriffen

Halten Sie Ransomware und unbekannte datenstehlende Malware von Ihrem Netzwerk fern. Leistungsstarke, cloudbasierte Next-Gen-Sandbox-Technologie und Deep Learning-Analyse zur schnellen und genauen Erkennung, Abwehr und Reaktion auf APTs und Zero-Day-Bedrohungen.

Einfache Implementierung

Sophos Sandstorm is komplett in Ihre Sophos-Sicherheitslösung integriert. Sie müssen nur 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. Unser systemübergreifender Emulationsansatz bietet einen detaillierten Einblick in das Verhalten unbekannter Malware und ermöglicht so die Erkennung von Malware-Angriffen, die andere einfach übersehen.

Forensik-Reports

Reagieren Sie mit einer einfachen, ereignisorientierten Analyse von Sicherheitsverletzungen schneller auf komplexe 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.

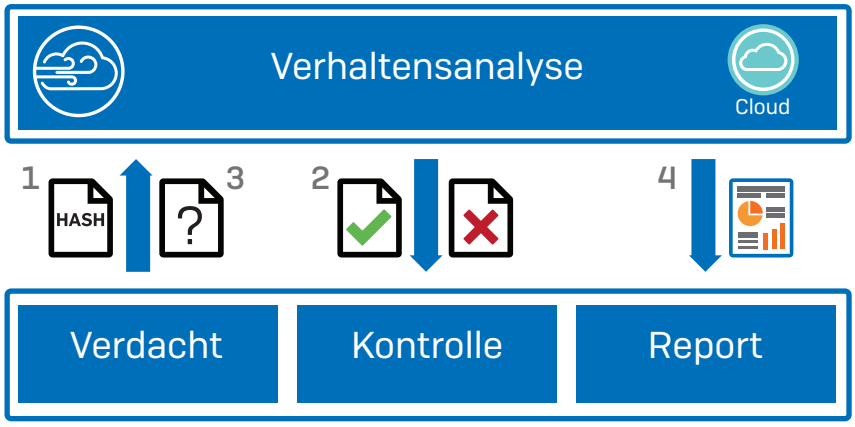
Blitzschnelle Performance

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 und Deep Learning zur Ausführung von Dateien in echten Umgebungen
- 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 behandelt. 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

03.01.2019 DS (PC)