



Solution Brief: Next- Generation Web Security

Von **Peter Craig**, Senior Product Marketing Manager

Das Internet ist und bleibt die Quelle Nummer 1 für Malware und 59 % davon lauert auf seriösen, vertrauenswürdigen Websites. Eine Next-Generation-Web-Security-Lösung muss umfassende Sicherheit, Transparenz und Kontrolle für alle Geräte Ihrer Benutzer bieten – egal, wie und wo diese auf das Internet zugreifen. Die Bereitstellung und Verwaltung müssen einfach sein und der Internetverkehr muss sich schnell und transparent ohne spürbare Performance-Einbußen analysieren lassen. Dieses Whitepaper beschreibt die zukunftsweisende Technologie von Sophos in den drei Kernbereichen der Next-Generation Web Security: erweiterte Sicherheit und Kontrolle; einfache Bedienung; Performance.

Erweiterte Sicherheit und Kontrolle

Die Art und Weise, wie Ihre Benutzer auf das Internet zugreifen, hat sich in den letzten Jahren grundlegend verändert. Sie arbeiten immer mobiler und verwenden dazu verschiedenste Geräte – einige werden vom Arbeitgeber zur Verfügung gestellt, andere gehören den Benutzern selbst. Auch auf was sie im Internet zugreifen, hat sich verändert. Mitarbeiter greifen immer häufiger auf cloudbasierte Anwendungen wie Dropbox und Facebook zurück, um ihre Arbeit effizienter zu erledigen – oft jedoch ohne Wissen oder Kontrolle der IT-Abteilung. Außerdem hat die Bedrohung durch Malware zugenommen. Angreifer setzen auf immer raffiniertere und zunehmend gezielte Bedrohungen, um herkömmliche Abwehrmaßnahmen zu überlisten. Verheerende Datenverluste und betriebsschädigende Ransomware-Payloads sind die Folge und gehören mittlerweile zum Alltag. Sophos Next-Generation Web Security wurde speziell entwickelt, um diesen Problemen entgegenzuwirken.

Einfache Bedienung

IT-Abteilungen in kleinen und mittelständischen Unternehmen stehen vor einer sehr schwierigen Aufgabe. Sie sind unterbesetzt und werden mit einer wachsenden Angriffsfläche sowie einer höheren Komplexität und Anzahl von Angriffen konfrontiert. Es ist daher wichtiger denn je, dass Ihre Sicherheitslösungen flexibel und intuitiv sind, und darüber hinaus auch weitreichende Konfigurationsmöglichkeiten bieten. Mit Sophos Next-Generation Web Security erhalten Sie die einfache Bedienung und Transparenz, die Sie benötigen. Die Lösung lässt sich mit all Ihren anderen Sophos-Produkten kombinieren und reduziert Ihren Verwaltungsaufwand erheblich, sodass Sie Ihre Zeit wichtigeren Aufgaben widmen können.

Performance

Beschwerden von Ihren Benutzern darüber, dass sich die Browsing-Geschwindigkeit verlangsamt hat, ist das Letzte, was Sie nach der Bereitstellung eines Web Security Service gebrauchen können. Ganz abgesehen von der Flut an Helpdesk-Anfragen, die Ihnen enorme Kopfschmerzen bereiten wird. Genau deshalb ist es so wichtig, dass eine Next-Generation-Web-Security-Lösung verlässliche Schutz- und Kontrollfunktionen mit niedriger Latenz bietet. Die Performance spielt auch beim Reporting eine wichtige Rolle. Die Lösung muss in der Lage sein, Reports zu generieren, mit denen Sie die Aktivitäten Ihrer Benutzer nachvollziehen können. Next-Generation-Lösungen, die die gebündelten Ressourcen der Cloud zur Bereitstellung von Reports nutzen, können ohne zeitliche Verzögerung Big Data Reporting liefern. Sophos Next-Generation Web Security bietet Ihnen schnelleres Web-Browsing durch eine verlässliche, global bereitgestellte Cloud-Infrastruktur sowie leistungsstarkes cloudbasiertes Reporting.

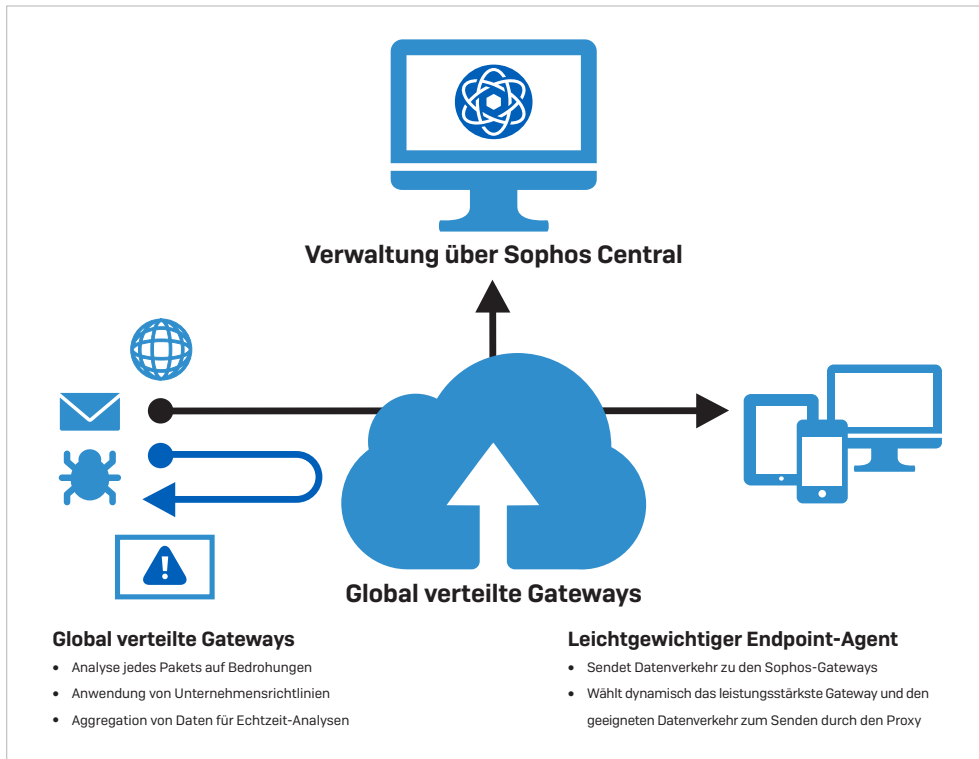
Sophos Web Gateway

Das Sophos Web Gateway ist eine Next-Generation-Web-Security-Lösung mit leistungsstarken Sicherheits- und Kontrollfunktionen, die sich einfach bereitstellen und verwalten lässt.

Das Sophos Web Gateway wird über die Cloud bereitgestellt und verwaltet. Die Verwaltung erfolgt über Sophos Central, die zentrale Konsole zur Verwaltung aller Ihrer Sophos-Produkte.

Leichtgewichtige Agenten werden auf jedem geschützten Gerät bereitgestellt. Diese senden den gesamten Internetverkehr durch ein Netzwerk zuverlässiger, global bereitgestellter Sophos-Gateways und wählen dynamisch das optimale Gateway und den richtigen zu scannenden Datenverkehr aus.

Jedes Paket wird auf Bedrohungen analysiert und die Richtlinien Ihres Unternehmens werden angewendet. Alle Daten werden protokolliert und für Echtzeit-Analysen aggregiert.



Erweiterte Sicherheit und Kontrolle

Erweiterte Sicherheit

Das Sophos Web Gateway nutzt SophosLabs-Daten über bekannte Malware-, „Command and Control“- und Exploit-Websites, um eine Navigation zu diesen Bedrohungsherden zu unterbinden. Zusätzlich ruft der Agent mittels Sophos Live Protection Echtzeit-Informationen über Schad-URLs ab. Die Liste der Schad-Websites wird ständig aktualisiert und die SophosLabs greifen zur Pflege ihrer Datenbank bekannter schädlicher Adressen sowohl auf selbst entwickelte Verfahren als auch auf Branchenfeeds zurück. Sophos verhindert nicht nur, dass der Browser zu einer verdächtigen Website navigiert, sondern scannt den Inhalt der Seite auch auf schädlichen Umleitungscode und kompromittierte Elemente (z. B. schädliche Flash-Objekte und Javascripts).

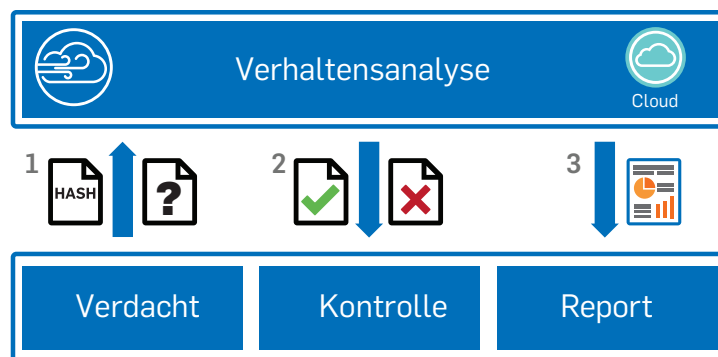
Sophos Web Security ermöglicht dies durch modernste Technologien wie JavaScript-Emulation, Verhaltensanalysen, kontextsensitive Überprüfungen und dynamische URL-Analysen für den HTTP- und HTTPS-Datenverkehr. Der Schutz beschränkt sich zudem nicht nur auf Web-Protokolle. Sophos Web Security scannt zusätzlich auch IMAP-, SMTP-, UDP- und DNS-Netzwerkverkehr und bietet somit umfassenden Schutz.

Next-Generation-Sandbox-Technologie

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 eine Next-Generation-Sandbox-Technologie, die gemeinsam mit Sophos-Web-Security-Lösungen genutzt werden kann. Sophos Sandstorm wird über die Cloud bereitgestellt und kann evasive Malware, die andere Lösungen übersehen (z. B. gezielte Malware und Ransomware), schnell und zuverlässig erkennen, blockieren und bekämpfen.

Wie funktioniert Sophos Sandstorm?

1. Enthält eine Datei bekannte Malware, wird sie sofort blockiert. Erscheint die Datei anderweitig verdächtig und ist bislang noch unbekannt, wird sie zur weiteren Analyse an die Sandbox gesendet. Kommt es durch die Analyse zu Verzögerungen beim Surfen im Internet, wird den Benutzern eine Meldung dazu angezeigt.
2. Die Datei wird in der sicheren Sandbox ausgeführt und auf schädliche Verhaltensweisen überwacht. Nach Abschluss der Analyse wird die Entscheidung, ob die Datei zugelassen oder blockiert werden soll, an die Sicherheitslösung übermittelt.
3. Für jede analysierte Datei wird ein detaillierter Report generiert.



Sicherheitsfunktionen

- Optionale Netzwerk-Sandbox Sophos Sandstorm
- Intelligente Scan-Engine scannt alle Web-Codes und -Skripte ohne Performance-Einbußen
- Mehrmals täglich automatische Bedrohungsupdates
- Echtzeitdaten zur Reputation von Websites
- Live Protection zur Echtzeitüberprüfung neuester Bedrohungen über die Cloud
- Automatische Erkennung anonymisierender Proxyserver in Echtzeit
- Identifizierung und Reporting für mehr als 500 Apps
- Scannt HTTP-, HTTPS-, IMAP-, SMTP-, UDP- und DNS-Netzwerkverkehr

Kontrolle

Sophos Web Security wurde speziell zur Kontrolle der Internet-Nutzung entwickelt. Mit den bereitgestellten Tools können Sie ganz einfach Richtlinien anpassen, um Compliance-Verpflichtungen nachzukommen, ein produktives Arbeiten ermöglichen, die Bandbreite optimieren, Anwendungen kontrollieren, Daten schützen und dafür sorgen, dass Ihre Benutzer und das Unternehmen sich sicher im Internet bewegen. Sophos bietet bereits seit vielen Jahren branchenführende Mobile-Device-Management- und Endpoint-Security-Lösungen an und hat auf Grundlage dieser Erfahrung eine Web-Security-Lösung entwickelt, die Benutzer überall und auf jedem Gerät schützt. Ganz gleich, ob Ihre Benutzer einen PC, Mac, ein iPad, iPhone oder Android-Gerät nutzen: Sie können stets sicher sein, dass Ihre Richtlinien überall durchgesetzt werden.

Der integrierte Endpoint-Agent verfügt über einen intelligenten Manipulationsschutz, setzt Ihre Richtlinien durch und stellt sicher, dass alle Benutzer richtlinienkonform bleiben.

Richtlinien- und Kontrollfunktionen

- Richtlinien nach Benutzern oder Gruppen
- Präzise Kontrollen für Cloud-Apps
- Mehr als 90 Website-Kategorien
- IP- und domainbasierte Gateway-Ausschlüsse
- Konfigurierbare SSL-Scans
- Konfigurierbare Datenschutzeinstellungen für Endbenutzer
- Detaillierte Application Control
- DLP erkennt Stichwörter, Datentypen (z. B. PII) und reguläre Ausdrücke
- DLP-Vorlagen erleichtern die Compliance mit PCI, Profanity (CIPA), HIPAA usw.

Einfache Bedienung

Die immer weiter wachsende Angriffsfläche und höhere Komplexität und Anzahl von Angriffen auf der einen Seite sowie kleine Teams und angespannte Arbeitsmärkte auf der anderen Seite stellen IT-Sicherheitsteams in Unternehmen vor große Herausforderungen. Vor dem Hintergrund dieses globalen Qualifikationsdefizits ist es wichtiger denn je, dass eine Next-Gen- Web-Security-Lösung einfach, flexibel und intuitiv ist. Sophos Web Security bietet all dies.

Einfach zu testen, bereitzustellen und zu verwalten

Da Sophos Web Gateway über die Cloud bereitgestellt wird, verkürzt sich für Sie der Zeitaufwand für den Test- und Bereitstellungsvorgang erheblich. Innerhalb von sechs Minuten nach Einrichtung eines Sophos Accounts verfügen Sie über ein voll funktionsfähiges Sophos Web Gateway und können den Datenverkehr in Ihrem Unternehmen filtern.

Ein weiteres Feature, mit dem sich das Sophos Web Gateway von anderen Produkten abhebt, ist seine vollständige Integration in Sophos Central. Sophos Central ist eine zentrale Konsole zur Verwaltung aller Ihrer Sophos-Produkte (Endpoint, E-Mail, Mobile, Server und Web) in einer Benutzeroberfläche. Sophos Central wurde so konzipiert, dass die leistungsstarken Richtlinieneinstellungen einfach und intuitiv sind. Mit den bereitgestellten Tools können Sie ganz

einfach Richtlinien anpassen, um Compliance-Verpflichtungen nachzukommen, ein produktives Arbeiten ermöglichen, die Bandbreite optimieren, Anwendungen kontrollieren, Daten schützen und dafür sorgen, dass Ihre Benutzer und das Unternehmen sich sicher im Internet bewegen.

Verwaltungsfunktionen

- Über webbasierte Sophos-Management-Konsole
- Kombinierte Verwaltung von Endpoint-, Mobil-, Server-, E-Mail- und Web-Sicherheit
- Verwaltung von Benachrichtigungen und Problemfällen

Bereitstellung und Verzeichnisdienst-Integration

- Unterstützung von Windows (7 und höher), OS X (10.8 und höher)
- iOS (4 und höher) und Android (4.0 und höher)
- Automatische Active-Directory-Synchronisation
- Manuelle Benutzereinrichtung mit automatischer Registrierung
- Hosting der Daten in Europa oder den USA

Performance

Das Sophos Web Gateway ist ein über die Cloud bereitgestellter Service mit zuverlässigen Webschutz- und Kontrollfunktionen und niedriger Latenz. Anstatt die Produktivität Ihrer Benutzer einzuschränken, kann die in die Endpoint-Agenten integrierte Sophos-Fastlane™-Technologie das Surfen im Internet durch intelligente Wiederverwendung von Verbindungen sogar beschleunigen.

Die Performance spielt auch bei der Report-Erstellung eine wichtige Rolle. Die Lösung muss Ihnen Reports liefern, anhand derer Sie die Aktivitäten Ihrer Benutzer nachvollziehen können. Next-Generation-Lösungen, die Ressourcen aus der Cloud zur Bereitstellung von Reports nutzen, können Big Data Reporting praktisch in Echtzeit generieren.

Schnell und leistungsstark

Bei Windows- und Mac-Endpoints ist das Sophos Web Gateway in den Endpoint integriert – auf diese Weise werden so wenig wie möglich Ressourcen beansprucht und die Performance wird aufrechterhalten. Alle unbekanntes Inhalte werden an die global bereitgestellte Cloud-Gateway-Infrastruktur von Sophos gesendet.

Bei mobilen Geräten wie Chromebooks und Android sendet der Endpoint-Agent den gesamten Datenverkehr mit geringem Endpoint-Verarbeitungsaufwand durch einen Proxy, um die Akkulaufzeit so wenig wie möglich zu beeinträchtigen. Der Agent wählt das optimale Gateway aus und nimmt kontinuierlich erneute Überprüfungen der Verbindungsleistung vor.

In allen Fällen ist die Verbindung vom Endpoint bis zum Gateway verschlüsselt, um den Schutz der Daten zu gewährleisten.

Das Sophos Web Gateway wird in einem globalen Netzwerk der Enterprise-Klasse gehostet, das für maximale Zuverlässigkeit rund um die Uhr kontrolliert wird. Unsere Rechenzentren sind durchweg SOC-2-konform und wir verbessern und erweitern unseren Service stetig, um Ihre Anforderungen noch effektiver zu erfüllen.

Performance-Features

- Global verteilte Infrastruktur
- „Fast Lane“-Technologie leitet Datenverkehr intelligent zum optimalen Sophos-Gateway weiter, um die Download-Geschwindigkeiten zu erhöhen
- 100%ige Netzwerkverfügbarkeit

Leistungsstarkes Reporting

Durch die Nutzung der Ressourcen unserer global bereitgestellten Cloud-Infrastruktur erhalten Sie mit dem Sophos Web Gateway Big Data Reporting – ohne lokalen Server oder zusätzliche Verwaltungskosten. Diese Reports liefern Ihnen eine Übersicht über Netzwerkanalysen, Anwendungen und Bedrohungen, um Ihre sensiblen Daten zu schützen, Kosten zu kontrollieren und Vorschriften einzuhalten.

Mit einfacher AD-Synchronisation lassen sich detaillierte Reports auf Benutzerebene zudem schnell erstellen. Oder nutzen Sie die Flexibilität, um anonyme Reports zur Internetnutzung durchzusetzen und auf diese Weise vor Ort geltenden gesetzlichen Vorschriften nachzukommen.

Reporting-Funktionen

- Über 100 verschiedene Reports zu Netzwerk und Bedrohungen
- Detaillierte Benutzer-Reports, u. a. nach Kategorie, Apps, Bedrohungen und Bandbreite
- Detaillierte Protokolle zu Netzwerkaktivitäten mit Quell- und Ziel-IP, URL, Protokoll, Port, ISP usw.
- Export von Reportdaten nach PDF oder CSV

Zusammenfassung

Next-Generation Web Security muss umfassende Sicherheit, Transparenz und Kontrolle für alle Geräte Ihrer Benutzer bieten – egal, wie und wo diese auf das Internet zugreifen. Die Bereitstellung und Verwaltung müssen einfach sein und der Internetverkehr muss sich schnell und transparent ohne spürbare Performance-Einbußen analysieren lassen.

Mit dem Sophos Web Gateway erhalten Sie umfassende Sicherheit, Transparenz und Kontrolle für alle Desktop-PCs, Macs, Chromebooks und mobilen Geräte. Das Sophos Web Gateway ermöglicht Ihren Mitarbeitern dank seiner Leistungsstärke ein ungestörtes Arbeiten und bietet mit Sophos Central eine einfache und elegante Verwaltung.

Testen Sie Sophos Web
Protection jetzt!

Kostenlose 30-Tage-Testversion unter
www.sophos.de/products/cloud-web-gateway

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

© Copyright 2016. 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.

SOPHOS