












Sophos-Produkte für den öffentlichen Sektor















Einrichtungen des öffentlichen Sektors sind für große Mengen vertraulicher Daten verantwortlich. Dies macht sie zu einem lohnenden Ziel für Cyberkriminelle. Wie gut Cyber-Angriffe abgewehrt werden können, hängt davon ab, wie umfassend die vorhandenen IT-Sicherheitslösungen sind und ob Firewalls und Endpoints in Echtzeit miteinander kommunizieren können. Außerdem muss die Cybersecurity-Infrastruktur in der Lage sein, Sicherheitslücken auf Netzwerk- oder Endpoint-Ebene zu schließen, die häufig für den Zugriff auf vertrauliche Daten ausgenutzt werden.










Sophos bietet für den öffentlichen Sektor eine Reihe leistungsstarker Cybersecurity-Lösungen, die umfassenden Schutz gewährleisten.











PROBLEM	SOPHOS-PRODUKT	FUNKTIONEN UND VORTEILE
Schutz für kritische und sensible Daten, die gespeichert sind (Data at Rest)	 Sophos XG Firewall  SG UTM  Sophos Intercept X	Die Data-Loss-Prevention (DLP)-Funktionen der Sophos-Produkte erkennen und verhindern das Abfließen kritischer Daten per E-Mail, Upload und Kopie.
	 Sophos Email Appliance  Sophos XG Firewall  SG UTM	Die Sophos SPX-Verschlüsselung wandelt E-Mail-Inhalte und -Anhänge dynamisch in ein sicheres, verschlüsseltes PDF um.
	 Sophos Mobile	Sophos Secure Workspace schützt Dokumente mit AES-256-Verschlüsselung. Sie ermöglicht eine sichere Verwaltung, Verteilung und Bearbeitung von Geschäftsdokumenten und die Anzeige von Web-Inhalten auf mobilen Geräten. Dank flexibler Compliance-Regeln lässt sich der Gerätestatus überwachen. Im Falle eines kompromittierten Geräts wird der Zugriff auf sensible Daten automatisch verweigert. E-Mails und Dokumente lassen sich im sicheren und verschlüsselten Sophos Container speichern. Der Zugriff ist über Sophos Secure Email und Sophos Secure Workspace möglich.
Schutz für kritische und sensible Daten während der Übertragung (Data in Transit)	 Sophos SafeGuard Encryption	Verschlüsselt gespeicherte Daten und Daten während der Übertragung auf Macs, Windows-Computern und mobilen Geräten. Verwaltet BitLocker- und FileVault-Festplatten-Verschlüsselungen sowie eine unterbrechungsfreie Dateiverschlüsselung für Daten auf Festplatten, USB-Sticks, Speicherkarten und CDs/DVDs oder in Cloud-Speichern und Netzlaufwerken. Die verschlüsselten Daten bleiben auch dann verschlüsselt, wenn sie im Netzwerk übertragen werden.
	 Sophos Wireless  Sophos XG Firewall  SG UTM	Erstellt dynamisch verschlüsselte WLAN-Verbindungen zum Schutz Ihrer Daten während der Übertragung in über Sophos Central verwalteten Netzwerken und Hotspots.

Sophos-Produkte für den öffentlichen Sektor

	 Sophos XG Firewall  SG UTM	Richtlinienbasierte Verschlüsselung für VPN-Tunnel schützt Daten während der Übertragung.
	 Sophos Email Appliance  Sophos XG Firewall  SG UTM	Sophos SPX Encryption verschlüsselt gespeicherte Daten und Daten während der Übertragung. Die SPX-Verschlüsselung wandelt E-Mail-Inhalte und -Anhänge dynamisch in ein sicheres, verschlüsseltes PDF um und stellt Compliance sicher.
Lateral Movement Protection – verhindert, dass Zugriff auf weitere Daten und Systeme erlangt wird	 Sophos XG Firewall	Isoliert und verhindert, dass Bedrohungen oder Angreifer sich lateral durch Ihr Netzwerk auf andere Systeme fortbewegen, selbst wenn sie sich in demselben Netzwerksegment oder derselben Broadcast-Domäne befinden, wo die Firewall normalerweise nicht eingreifen kann. Auf diese Weise lassen sich aktive Angreifer in Ihrem Netzwerk sehr einfach und effektiv bekämpfen.
Nahtloser Informationsaustausch zwischen Endpoint und Firewall	 Synchronized Security in Sophos-Produkten	Ermöglicht durch den Austausch von Telemetrie- und Statusdaten ein koordiniertes Erkennen, Isolieren und Beseitigen von Malware auf Servern, Endpoints und Firewalls. So können auch komplexe Angriffe gestoppt werden.
Umfangreiche und einfache zentrale Verwaltungsfunktionen	 Sophos Central	Alle Sophos-Produkte lassen sich über dieselbe, zentrale Benutzeroberfläche verwalten. Die Remote-Verwaltung und Bereitstellung aller Sophos-Produkte ist über eine zentrale, cloudbasierte Management-Konsole möglich.
Stoppen von Phishing-Angriffen, bevor sie in den Posteingang Ihrer Mitarbeiter gelangen	 Sophos Email	Automatisiert den Phishing-Schutz mittels Authentifizierung. Schützt Ihre Mitarbeiter bereits vor der E-Mail-Zustellung vor Phishing-Angriffen, bei denen die E-Mails vermeintlich von bekannten Kontakten oder Domains stammen. Dank der Kombination aus SPF-, DKIM- und DMARC-Authentifizierungstechniken und E-Mail-Header-Analysen können Sie mit Sophos Email legitime E-Mails von bekannten Kontakten klar erkennen und zulassen und betrügerische E-Mails blockieren.
	 Sophos Phish Threat	Mit Sophos Phish Threat können Sie Phishing-Cyber-Angriffe simulieren und Ihren Endbenutzern Security-Awareness-Trainings bieten. Die Trainings decken verschiedenste Bereiche ab, u. a. bieten sie allgemeine Infos zu Phishing und Cybersecurity. Sie behandeln aber auch spezielle Themen zu IT-Trainings, Compliance, Malware, Risiken im Zusammenhang mit Mobilgeräten, Passwort-Schutz etc.
Blockieren von verdächtigen/schädlichen URLs und Bedrohungen aus dem Internet	 Sophos XG Firewall  SG UTM	<p>Sie profitieren von einem vollständig transparenten Proxy für Anti-Malware und Web-Filtering sowie von einer URL-Filterdatenbank mit Millionen von Websites aus über 90 Kategorien, die von einer kontinuierlich aktualisierten Datenbank der SophosLabs gespeist wird.</p> <p>Unsere moderne Web Protection Engine scannt Web-Inhalte intelligent und blockiert die neuesten Web-Bedrohungen mithilfe modernster Techniken wie JavaScript-Emulation, Verhaltensanalyse, kontextsensitiver Überprüfung und dynamischer URL-Analyse für HTTP- und HTTPS-Datenverkehr.</p>

Sophos-Produkte für den öffentlichen Sektor

Schutz vor Ransomware und sonstigen Arten komplexer Malware	 Sophos Intercept X  Sophos Intercept X for Server	<p>Anti-Exploit, Anti-Ransomware und Deep-Learning-Malware-Erkennung schützen Endpoints vor ausführbarem Schadcode.</p> <p>Integriert innovative Technologien wie Deep Learning, Anti-Exploit und Adversary Mitigation in Malicious Traffic Detection, mit Echtzeit-Bedrohungsdaten. So können Sie Bedrohungen einfach abwehren, erkennen und beseitigen.</p> <p>Nach einem Ransomware-Angriff oder Angriff auf den Master Boot Record werden alle Dateien in ihren Ursprungszustand zurückversetzt. Sophos Clean entfernt dank forensikbasierter Bereinigungsfunktionen sowohl den Schadcode als auch die von der Malware erstellten Registry-Schlüssel-Änderungen.</p>
	 Sophos Mobile	<p>Mit Unified Endpoint Management (UEM) und der Security-Verwaltung für traditionelle und mobile Endpoints wird die Integrität von sensiblen Daten gewahrt sowie Geräte und Benutzer geschützt. Sophos Mobile Security bietet Mobile Threat Defense-Funktionen für Android und iOS mit Sicherheitsfunktionen für Geräte, Apps und Netzwerke: erstklassiger Schutz vor Malware und Ransomware mit leistungsstarker Deep Learning-Technologie für Android-Geräte.</p>
	 Sophos XG Firewall	<p>Umfasst APT und Sandboxing mit Deep Learning zur Überwachung und Blockierung von eingehendem oder ausgehendem schädlichen Internetverkehr. Sophos Sandstorm, unsere cloudbasierte Sandbox-Technologie, analysiert und blockiert Executables und Dokumente mit ausführbarem Inhalt, bevor die Datei auf das Gerät des Benutzers gelangt.</p>
	 Synchronized Security in Sophos-Produkten	<p>Ermöglicht durch den Austausch von Telemetrie- und Statusdaten ein koordiniertes Erkennen, Isolieren und Beseitigen von Malware auf Servern, Endpoints und Firewalls. So können auch komplexe Angriffe gestoppt werden.</p>
	 Sophos Email Appliance	<p>Auf Grundlage von Echtzeit-Bedrohungsdaten aus den SophosLabs werden unerwünschte E-Mails direkt am Gateway erkannt und blockiert und unsere Anti-Spam-Engine fängt alle übrigen Bedrohungen ab – selbst neueste Phishing-Angriffe, schädlichen Anhänge und Snowshoe-Spam.</p>
Schutz vor internen Bedrohungen	 Sophos XG Firewall	<p>Der User Threat Quotient (UTQ) hilft bei der Erkennung von Benutzern, die aufgrund ihres verdächtigen Verhaltens im Internet sowie ihres Bedrohungs- und Infektionsverlaufs ein Risiko darstellen. Hohe UTQ-Risikobewertungen von Benutzern können auf unbeabsichtigtes Fehlverhalten infolge mangelnden Sicherheitsbewusstseins, eine Malware-Infektion oder bewusstes Fehlverhalten hindeuten.</p>
	 Sophos XG Firewall  SG UTM	<p>Nutzersensibilisierung in allen Bereichen unserer Firewall bildet die Grundlage für alle Firewall-Richtlinien und Reports und ermöglicht eine benutzer- oder gruppenbasierte Next-Gen-Kontrolle über Anwendungen, Websurfen, Bandbreitenkontingente und weitere Netzwerkressourcen. Die Sophos XG Firewall mit Security Heartbeat™ ermöglicht es, dass Next-Gen Endpoint und Network Security kontinuierlich wichtige Informationen zu verdächtigen Ereignissen im gesamten erweiterten IT-System miteinander austauschen. Dadurch werden kompromittierte/nicht autorisierte Endpoints nahezu in Echtzeit automatisch erkannt und isoliert. So wird verhindert, dass von ihnen vertrauliche Daten abfließen.</p>

	 Sophos SafeGuard Encryption	<p>Authentifiziert Benutzer für den Zugriff auf bestimmte geschützte Geräte, Dateien und/oder Ordner mit benutzer- oder gruppenspezifischen Schlüsseln. Unterstützt mehrstufige Authentifizierung, Token und Smart Cards zur Benutzerauthentifizierung.</p> <p>Unterstützt das Risikomanagement durch Authentifizierung von Benutzern für den Zugriff auf bestimmte Dateien/Ordner mithilfe benutzer- oder gruppenspezifischer Verschlüsselungsschlüssel.</p>
	 Sophos Central	<p>Schützt privilegierte und Administrator-Konten dank erweiterter Zwei-Faktor-Authentifizierung: Zugriffslisten und Informationen über Benutzerberechtigungen sind stets auf dem neuesten Stand. Kontrolle für Zugriffsrechte: Erfüllen Personen nicht mehr die Voraussetzungen für Zugriffsrechte, werden ihnen ihre Zugriffsrechte entzogen (z. B. weil sie die Stelle wechseln oder das Unternehmen verlassen).</p>
	 Sophos Mobile	<p>Sophos Secure Email und Sophos Secure Workspace in Sophos Mobile speichern Daten sicher auf mobilen Geräten mit AES-256-Verschlüsselung. Der Zugriff auf die Inhalte in den Apps kann basierend auf Gerätestatus, Compliance-Regeln, Zeit, WLAN oder Geolokation eingeschränkt werden.</p>
<p>Ausweitung der unternehmensseitigen IT-Sicherheit über die Netzwerkgrenze hinaus: mobile Mitarbeiter und Zweigstellen</p>	 Sophos Mobile	<p>Bietet Enterprise Mobility und Security-Verwaltung für traditionelle und mobile Endpoints einschließlich Sicherheits- und Geräterichtlinien. Dank flexibler Compliance-Regeln lässt sich der Gerätestatus überwachen. Im Falle eines kompromittierten Geräts wird der Zugriff auf sensible Daten automatisch verweigert. E-Mails und Dokumente lassen sich im sicheren und verschlüsselten Sophos Container speichern. Der Zugriff ist über Sophos Secure Email und Sophos Secure Workspace möglich. Die Sophos Secure Workspace App schützt sensible Daten mit AES-256-Verschlüsselung. Sie ermöglicht eine sichere Verwaltung, Verteilung und Bearbeitung von Dokumenten und die Anzeige von Web-Inhalten auf mobilen Geräten.</p>
	 Sophos XG Firewall  SG UTM	<p>Ermöglicht eine Zwei-Faktor-Authentifizierung für VPN-Verbindungen, mit RADIUS/TACACS-Integration.</p> <p>Dank Sophos RED (Remote Ethernet Device) können Sie einen sicheren Ethernet-Tunnel aufbauen und so Ihr sicheres Netzwerk ganz einfach auf einen Remote-Standort ausweiten.</p>
	 Sophos SafeGuard Encryption	<p>Verschlüsselt gespeicherte Daten und Daten während der Übertragung auf Macs, Windows-Computern und mobilen Geräten. Verwaltet BitLocker- und FileVault-Festplatten-Verschlüsselungen sowie eine unterbrechungsfreie Dateiverschlüsselung für Daten auf Festplatten, USB-Sticks, Speicherkarten und CDs/DVDs oder in Cloud-Speichern und Netzlaufwerken. Die verschlüsselten Daten bleiben auch dann verschlüsselt, wenn sie im Netzwerk übertragen werden.</p>
	 Sophos Email Appliance  Sophos XG Firewall  SG UTM	<p>Sophos SPX Encryption verschlüsselt gespeicherte Daten und Daten während der Übertragung. Die SPX-Verschlüsselung wandelt E-Mail-Inhalte und -Anhänge dynamisch in ein sicheres, verschlüsseltes PDF um und stellt Compliance sicher.</p>

Sophos-Produkte für den öffentlichen Sektor

Schutz der Netzwerkintegrität	 Sophos XG Firewall  SG UTM	Dank rollenbasierter Verwaltung lässt sich die Verwaltung Ihrer Netzwerksicherheit delegieren. Datenverkehr, Services, Ports und Protokolle werden blockiert mit Ausnahme explizit zugelassener Anwendungen und als für das Unternehmen geeignet und erforderlich definiert.
	 Sophos Mobile	Die Integration mit Sophos UTM, Sophos Wireless Access Points und anderen UTMs ermöglicht eine integrierte, konsistente Sicherheit und Compliance-Durchsetzung für mobile Geräte, die auf das Netzwerk und andere Dienste zugreifen.
	 Sophos Intercept X  Sophos Intercept X for Server	Eine Kombination aus HIPS-Technologie, Deep Learning, Anti-Exploit, Active Adversary Protection und Malicious Traffic Detection erkennt proaktiv schädliches Verhalten auf dem Host.
Einhaltung globaler Best Practices wie NIST Cybersecurity Framework, NIS-Richtlinie etc.	 Alle Sophos-Produkte	Security-Produkte von Sophos helfen Einrichtungen des öffentlichen Sektors, von ihnen erwartete Best Practices für Cybersecurity-Compliance umzusetzen. Weitere Informationen finden Sie auf der Compliance-Seite von Sophos .
Sicherheit für die Cloud-Infrastruktur	 Sophos Cloud Optix	Als KI-basierte Next-Gen Security-Plattform für die Cloud-Infrastruktur ermöglicht Sophos Cloud Optix eine kontinuierliche Sicherheitsüberwachung, Compliance, Analyse und Bereinigung – und zwar für mehrere verschiedene Public-Cloud-Konten und -Plattformen.

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

© Copyright 2019. 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.

2019-05-09 RC (PC)

SOPHOS