Sophos Intercept X for Mobile

Mobile Threat Defense (MTD) für Android-, iOS- und Chrome-OS-Geräte

Sophos Intercept X for Mobile schützt mit unserer marktführenden Intercept X Deep Learning Engine Benutzer, Geräte und Unternehmensdaten vor bekannten und unbekannten Bedrohungen. Die gesamte Verwaltung erfolgt nahtlos über Sophos Central, gemeinsam mit allen anderen Next-Generation-Cybersecurity-Lösungen des Sophos-Portfolios.

Gerätesicherheit

Sophos Intercept X for Mobile überwacht kontinuierlich den Gerätestatus und informiert Sie bei einer Kompromittierung, damit Sie eine Bereinigung einleiten oder den Zugriff auf Unternehmensressourcen automatisch sperren können. Der Security Advisor des Geräts erkennt Jailbreaking oder Rooting und kann den Benutzer und Admin über notwendige Betriebssystem-Updates informieren.

Netzwerksicherheit

Sie erhalten eine erste Verteidigungslinie für mobile Android- und iOS-Geräte. Netzwerkverbindungen werden in Echtzeit auf verdächtige Merkmale überprüft, die auf einen Angriff hindeuten könnten. So lässt sich die Anfälligkeit für Man-in-the-Middle (MitM)-Angriffe verringern. Web- und URL-Filter verhindern den Zugriff auf bekannte schädliche Websites, und die SMS-Phishing-Erkennung entlarvt schädliche URLs.

Anwendungssicherheit

Sophos Intercept X for Mobile erkennt dank Deep Learning und Daten der SophosLabs schädliche und potenziell unerwünschte Anwendungen auf Android-Geräten. Ändert sich der Bedrohungsstatus eines Geräts, werden Benutzer und Admins benachrichtigt. Durch die Integration mit Microsoft Intune können Admins Richtlinien für eingeschränkten Zugriff festlegen und so den Zugriff auf Apps und Daten beschränken, wenn eine Bedrohung erkannt wird.

Zentrale Bereitstellung, Konfiguration und Reporterstellung

Sophos Intercept X for Mobile lässt sich zentral über Sophos Central konfigurieren, wo unsere Unified Endpoint Management (UEM)-Plattform gehostet wird. Die Bereitstellung der App erfolgt über einen App Store (Anmeldung erforderlich) oder über UEM-Produkte wie Sophos Mobile oder Enterprise Mobility Management (EMM)-Produkte von Drittanbietern.

Bedingter Zugriff mit Synchronized Security

Sophos Synchronized Security ermöglicht Ihren Abwehrmaßnahmen, als System zusammenzuarbeiten und koordinierter zu agieren als die Angreifer. Informationen zum Bedrohungsstatus können mit Sophos Wireless Access Points ausgetauscht werden. So stellen Sie sicher, dass alle Geräte bereinigt sind, bevor sie Zugriff auf sensible Netzwerke erhalten.

Highlights

- Schutz für Android-, iOS- und Chrome-OS-Geräte
- Bereitstellung über Sophos Central oder andere UEM-Produkte
- Nutzt auf Android Sophos Intercept X mit Deep Learning
- Umfassende Man-in-the-Middle (MitM)-Bedrohungserkennung
- Preisgekrönte Mobile Threat Defense
- Bedingter Zugriff mit Microsoft Intune
- Im Apple App Store und Google Play Store erhältlich

SOPHOS

Features

LIZENZ	ANDROID	IOS	CHROME OS
ALLGEMEINES			
Management-Konsole	Sophos Central	Sophos Central	Sophos Central
Partner Dashboard für Managed Service Provider	✓	✓	✓
Produktinterne Unterstützung von Mehrinstanzenfähigkeit	✓	✓	✓
Microsoft Active Directory oder Azure AD Integration	✓	✓	✓
GERÄTESICHERHEIT			
Erkennung von Rooting/Jailbreak	✓	✓	
Überprüfung Betriebssystem-Version	✓	✓	✓
Upgrade-Advisor Betriebssystem	✓		
NETZWERKSICHERHEIT			
Erkennung MitM-Angriff	✓	✓	
Web-Schutz vor schädlichen Online-Inhalten	✓[1]	✓[2]	✓
Web-Filterung nach unerwünschten Inhalten (14 Kategorien)	✓[1]	✓[2]	✓
Phishing-Schutz vor URLs in Textnachrichten	✓	✓	
ANWENDUNGSSICHERHEIT			
Schutz vor Malware und Ransomware (signaturbasiert und mittels Deep Learning)	✓		
Erkennung potenziell unerwünschter Apps (PUA)	✓		
App-Reputation	✓		
Erkennung nicht aus dem App Store installierter Apps		✓[3]	✓
ZUSÄTZLICHE SICHERHEITSFUNKTIONEN			
Sicherer QR-Code-Scanner	✓	✓	
Password Safe	✓	✓	
Authentifizierung (TOTP und HOTP)	✓	✓	
Privacy Advisor	✓		
Security Advisor (z.B. Side Loading, Geräte-Verschlüsselung)	✓		
SYSTEMINTEGRATION			
Bereitstellung mit Fremd-EMM-Lösungen möglich	✓[4]	✓	✓
Intune Conditional Access Integration	✓	✓	
SIEM-Integration	✓	✓	✓
Synchronized Security mit Sophos Wireless	✓	✓	

1 Nicht unterstützt bei Bereitstellung innerhalb von Android Enterprise Work Profile
2 iOS-betreute Geräte erforderlich
3 Nur in Kombination mit Sophos Mobile
4 Verwaltete Android-Enterprise-Geräte erforderlich (kein Device Admin Management)

Download on the App Store

App Store und das App Store Logo sind Marken von Apple Inc.

JETZT BEI Google Play

Google Play und das Google Play Logo sind Marken von Google LLC.

Intercept X for Mobile jetzt kostenlos herunterladen

Erhältlich im Google Play Store und Apple App Store

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

SOPHOS

21-04-16 DS-DE (PS)