

# Sophos Intercept X for Mobile



## Mobile Threat Defense (MTD) for Android, iOS and Chrome OS devices

Intercept X for Mobile protects users, their devices, and corporate data from known and never-before-seen mobile threats by leveraging our market leading Intercept X deep learning engine. It is all managed seamlessly through Sophos Central, alongside the entire Sophos portfolio of next-generation cybersecurity solutions.

### Device security

Sophos Intercept X for Mobile continuously monitors device health and notifies you if a device is compromised so you can take remediating action or automatically revoke access to corporate resources. Device security advisors detect jailbreaking or rooting and can inform the user and admin of necessary operating system updates.

### Network security

Establish a first line of defense at the mobile network level on Android and iOS. Network connections are examined in real time to check for suspicious characteristics that may identify an attack. This helps mitigate the risk of Man-in-the-Middle (MitM) attacks. Web filtering and URL checking stops access to known bad sites on mobile devices, while SMS phishing detection spots malicious URLs.

### Application security

Sophos Intercept X for Mobile detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Users and admins are notified if the threat status of a device changes. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.

### Centralized deployment, configuration, and reporting

Sophos Intercept X for Mobile can be centrally configured from Sophos Central, which hosts our Unified Endpoint Management (UEM) platform. Deployment can occur via existing app stores with user enrolment, or the app can be pushed using existing UEM's such as Sophos Mobile or third-party Enterprise Mobility Management (EMM) tools.

### Conditional access with Synchronized Security

Synchronized Security enables your defenses to work together as a system to be more coordinated than the attackers. Threat status information can be shared with Sophos Wireless access points to ensure all threats on devices are fully remediated before access to sensitive networks is granted.

### Highlights

- Protection for Android, iOS, and Chrome OS devices
- Deploy using Sophos Mobile or alternate UEM products
- Leverages Intercept X deep learning on Android
- Comprehensive Man-in-the-Middle (MitM) threat detection
- Award-winning mobile threat defense
- Microsoft Intune conditional access
- Available from the Apple App Store and Google Play Store

## Features

| LICENSE                                                                      | ANDROID        | IOS            | CHROME OS      |
|------------------------------------------------------------------------------|----------------|----------------|----------------|
| <b>GENERAL</b>                                                               |                |                |                |
| Management console                                                           | Sophos Central | Sophos Central | Sophos Central |
| Partner Dashboard for Managed Service Providers                              | ✓              | ✓              | ✓              |
| In-product multi-tenant support                                              | ✓              | ✓              | ✓              |
| Microsoft Active Directory or Azure AD integration                           | ✓              | ✓              | ✓              |
| <b>DEVICE SECURITY</b>                                                       |                |                |                |
| Rooting/jailbreak detection                                                  | ✓              | ✓              |                |
| OS version check                                                             | ✓              | ✓              | ✓              |
| OS upgrade advisor                                                           | ✓              |                |                |
| <b>NETWORK SECURITY</b>                                                      |                |                |                |
| MitM attack detection                                                        | ✓              | ✓              |                |
| Web protection against malicious online content                              | ✓ <sup>1</sup> | ✓ <sup>2</sup> | ✓              |
| Web filtering for unwanted content [14 categories]                           | ✓ <sup>1</sup> | ✓ <sup>2</sup> | ✓              |
| Phishing protection from URLs in text messages                               | ✓              | ✓              |                |
| <b>APPLICATION SECURITY</b>                                                  |                |                |                |
| Protection against malware or ransomware [Signature and Deep Learning based] | ✓              |                |                |
| Potentially unwanted apps (PUA) detection                                    | ✓              |                |                |
| App reputation                                                               | ✓              |                |                |
| Detect non-App Store apps                                                    |                | ✓ <sup>3</sup> | ✓              |
| <b>ADDITIONAL SECURITY FEATURES</b>                                          |                |                |                |
| Secure QR code scanner                                                       | ✓              | ✓              |                |
| Password safe                                                                | ✓              | ✓              |                |
| Authenticator (TOTP and HOTP)                                                | ✓              | ✓              |                |
| Privacy advisor                                                              | ✓              |                |                |
| Security advisor (e.g. side loading, device encryption)                      | ✓              |                |                |
| <b>SYSTEM INTEGRATION</b>                                                    |                |                |                |
| Support for rollout with 3rd party EMM solutions                             | ✓ <sup>4</sup> | ✓              | ✓              |
| Intune Conditional Access integration                                        | ✓              | ✓              |                |
| SIEM integration                                                             | ✓              | ✓              | ✓              |
| Synchronized Security with Sophos Wireless                                   | ✓              | ✓              |                |

1 Not supported if deployed inside Android Enterprise Work Profile

2 Requires iOS supervised devices

3 Only in combination with Sophos Mobile

4 Requires Android Enterprise managed devices (no Device Admin management)



App Store and App Store logo are trademarks of Apple Inc.



Google Play and the Google Play logo are trademarks of Google LLC.

## Download Intercept X for Mobile now for free.

Available on Google Play and Apple App Stores

United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: [sales@sophos.com](mailto:sales@sophos.com)

North American Sales  
Toll Free: 1-866-866-2802  
Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Asia Sales  
Tel: +65 62244168  
Email: [salesasia@sophos.com](mailto:salesasia@sophos.com)