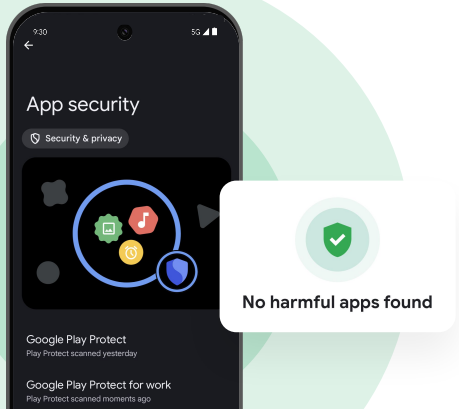
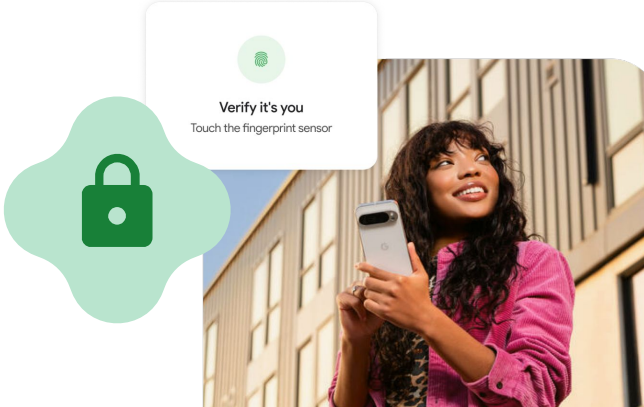
Android

The Mobile Security Guidebook for SMBs





Overview

Implementing robust data security is especially key for small businesses. According to Hiscox[1], 25% of small businesses go out of business after a security breach, for which the average cost is $200K.

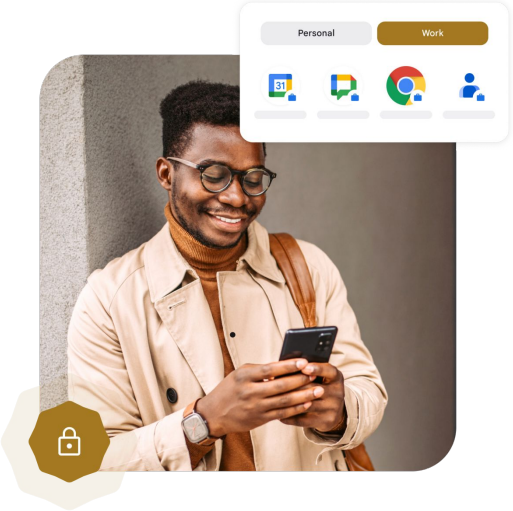
In today's hyper-connected world, your smartphones and tablets are both a powerful tool and a potential security risk if not properly managed.

One of the largest threats to mobile users is phishing, with 83% of phishing sites[2] targeting mobile devices specifically. Attackers are now using AI to craft sophisticated attacks that can fool even experienced users.

Managing the full life cycle of business devices and ensuring the security and privacy of employee and company data may seem like a complex task, but it can be easy and simple with the right tools.

Android offers simple, unobtrusive security protections, to help secure company devices and data and defend from phishing attacks. This is especially critical for businesses where there may not be dedicated IT support to secure and manage devices.

In this guide we share best practices to safeguard your business data, and reinforce what makes Android such a robust and secure platform.



[1] Hiscox Cyber Readiness Report
[2] Zimperium's 2024 Global Mobile Threat Report

Understanding Android device enrollment models

There are three specific directions, or models, businesses could take in securing devices and data. Each model increases the amount of control IT teams have over a device.

01

The first model, which has no Enterprise Mobility Management (EMM) or management functions, is classified as User Initiated. In this model, the company's IT team educates and guides users on best practices to configure specific security and privacy settings on a user's device.

02

For the second model, Device Trust from Android Enterprise offers a zero trust based model for enhanced security. This approach improves the ability for trusted solution providers to inspect the security state of a device independent of the device being managed by an EMM. These include a broad set of solutions including Identity providers (IdPs), Mobile Threat Defense (MTDs), Enterprise Detection and Response (EDRs), and Virtual Private Network providers (VPNs). Integration with Android Enterprise allows these partner solutions to be able to verify that specific device criteria are met before granting access to company resources.

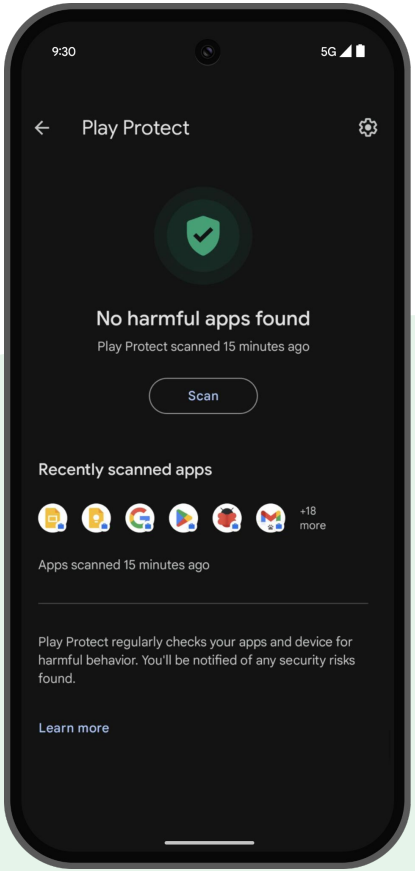
03

The third model relies on Enterprise Mobility Management (EMM) controls, enabling organizations to exert greater control over user devices, whether company-owned or part of a Bring Your Own Device (BYOD) program. In the case of personal devices, the company enrolls a Work Profile, granting IT comprehensive control over all facets of this profile while preserving user privacy in their personal area.

Android Enterprise offers several device enrollment models to meet the needs of SMB customers

Each model builds on top of each other to provide SMBs with flexibility and all can be used together as per business need. Leveraging Android's robust security features and implementing the following best practices will allow your business to confidently operate in the mobile environment.

Android's commitment to security advancements, along with its flexibility and cost-effectiveness, positions it as the optimal selection for small and midsize businesses.



Security policies & settings recommended for enrollment models

Specific guidance for each model: User Initiated, Device Trust, and EMM.

Each of these models is geared towards a specific level of user privacy and company control based on your level of requirements.

01 User initiated security settings

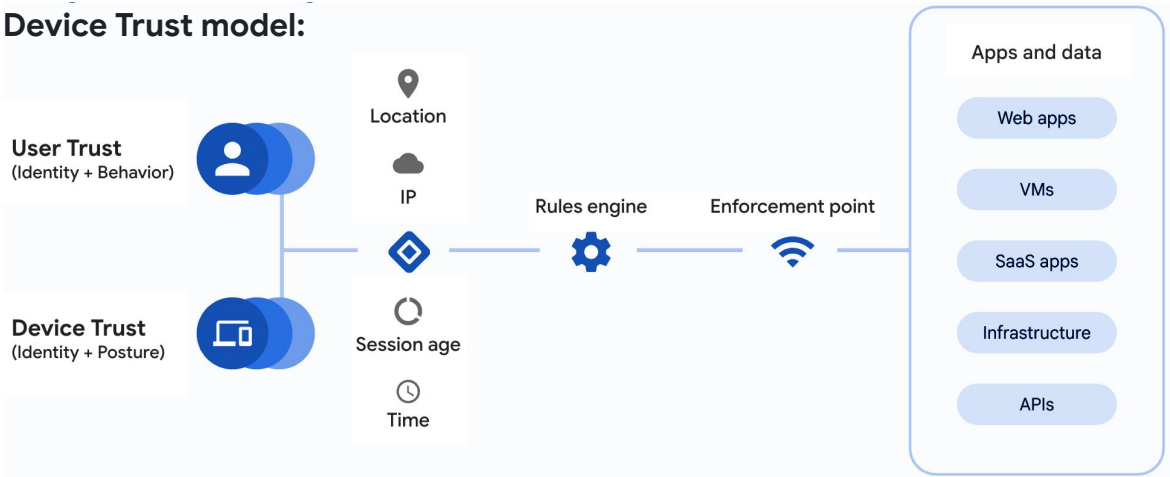
IT team will provide instructions for users on how and why they should manually setup the following settings on their Android Devices to help protect the users and the company's data.

- Enable Theft Detection Lock
- Enable Remote Lock
- Enable Offline Device Lock
- Enable Identity check
- Enable private space
- Set a pin or passcode that is at least 6 characters and non-repeating
- Ensure that Google Play Protect is enabled
- Only install apps from Google Play Store

02 Zero Trust Model

In addition to the available controls & restrictions with Device Trust by Android Enterprise, IT should also instruct users to setup and take advantage of all the User Initiated security features in section 1.

Device Trust model:



Decide from the following list what checks you want to implement before allowing access to company assets. Choice of settings will be dependent on Device Trust Partners, please see their documentation.

02 Device Trust from Android Enterprise

Decide from the following list what checks you want to implement before allowing access to company assets. Choice of settings will be dependent on Device Trust Partners, please see their documentation.

Signal	Description
Device model or brand	Returns the device model and brand.
Management state	Returns the management and the management app.
Network state	Returns information about all active networks on the device.
Device security patch level	Returns the current security patch level of the device (including the Play System Update patch level).
Published security patch level	Returns the security patch level published by Google for the corresponding updatable component on the device.*
Disk encryption status	Returns if the device storage is encrypted.
OS version and pending OTA	Returns the OS version of the device and if there is a pending OS update available.
Screen lock and quality check	Returns the complexity of the user's current screen lock.
Play Protect status	Returns if the Google Play Protect is enabled.

03 Enabled by EMM policies

IT admins can refer to their EMM documentation on how to set up these minimal sets of policies to protect users. Using an EMM allows IT to set up devices as Work Profile only, Corporate Owned, Personally Enabled (COPE), or Fully Managed. Both Work Profile and COPE provide a means for the Company to control a work profile, with only COPE providing more control over the entire device. Here are some examples of security controls that should be considered:

- Minimum password length = 6 characters
- Max attempts to unlock the device = 10
- Enable Google Play Integrity
- Disable screenshots
- Disallow adding accounts in Work Profile
- Disable Developer Options
- Disallow install from unknown sources
- Disable cross-profile copy/paste
- Disallow Android Debug Bridge (ADB)
- Use managed Google Play with allowlists
- Chrome: Prevent disabling Safe Browsing

Best practices for deploying Android devices in your business

01 Educate and instruct employees to enable built-in security capabilities

Best Practice

Help protect your data from thieves and unauthorized access with additional built-in features that are designed to secure confidential business information. These include:

A

Turn on Theft Detection Lock which uses AI, your device's motion sensors, Wi-Fi, and Bluetooth to detect a snatch motion and locks the device automatically.

B

Turn on & use Remote Lock.
If your device is lost or stolen, to quickly lock your screen, you can use Remote Lock with a verified phone number.

C

Turn on Offline Device Lock. After your device goes offline, Offline Device Lock automatically locks your device screen to help protect your data. For example, if someone steals your phone and turns off the internet to prevent you from finding it with Find My Device, your device locks after a short period of being used offline.

01 Educate and instruct employees to enable built-in security capabilities

Best Practice

Help protect your data from thieves and unauthorized access with additional built-in features that are designed to secure confidential business information. These include:

D

Turn on Identity Check. To verify your identity, Identity Check requires biometrics and other safeguards. Your identity gets verified when you perform sensitive actions on your device or make changes to your Google Account outside trusted places.

E

Hide sensitive apps with private space. To safeguard your private applications from unauthorized access, Android offers a "private space" feature. This creates a distinct, hidden area on your device where you can organize your personal apps. Even if your unlocked phone falls into the wrong hands, your sensitive applications within the private space will remain protected.

F

Google has also integrated anti-phishing capabilities directly into Google Messages to help protect users from sophisticated phishing techniques. Additionally, there are new features such as spam protection and Android caller ID to further enable user protection.

02 Use the Android Enterprise Recommended Solutions Directory

Best Practice

Create a list of approved devices for use at work from the Android Enterprise Recommended solutions directory.

The devices in our solutions directory undergo rigorous security testing and receive timely updates.

Android Enterprise Recommended validation ensures your business gets devices with built-in security enhancements and features that are optimized for business needs.

03 Deploy a Device Management Solution for Centralized Control

Best Practice

Utilize an EMM (Enterprise Mobility Management) solution to enforce security policies, remotely wipe/lock devices, and manage application installations. To find a list of validated and approved EMM partners you can visit the Android Enterprise Recommended EMM Solutions Directory.

Android's deep integration with EMM solutions allows for granular control and efficient security management for any size company.

04 Ensure timely security updates

Best Practice

Use Android Enterprise device policies via an EMM to ensure all devices are updated with the latest Android security patches. Android Enterprise enables Admins with options to enforce OS and Application update policies that meet company needs.

Android has committed to regular security updates every 30 days so the ecosystem of device makers and carriers can deliver updates fast. Additionally, if you select devices from the Solutions Directory, those devices are required to deliver updates at least every 90 days. Device makers, for example Pixel and Samsung, are now delivering 7 years of OS and security updates. This will help ensure potential vulnerabilities are patched quickly.

05 Implement Strong Authentication

Best Practice

Android Enterprise controls provides the capability to set requirements for device unlock pass codes. These include pins, patterns, and passcodes which can be coupled with fingerprint and face unlock as options. Admins can require users to set specific requirements that meet the organization's needs. Be sure to require at least 6 digits with non-repeating characters, in accordance with the latest guidelines from NIST SP 800-53.

Android's biometric support coupled with secure key storage provides users with a seamless experience and helps protect your device with robust hardware backed secure authentication.

06 Securely Deploy and Manage Applications

Best Practice

Only permit users to install applications from the Google Play Store and require Google Play Protect to always be enabled. Using Managed Google Play allows Admins to collate a list of approved apps and set permissions.

Managed Google Play prevents sideloading unapproved applications and Google Play Protect actively scans all installed applications for malware.

07 Protect Data in Transit

Best Practice

Use VPNs for secure connections to business services while away from the office, ensure all services are using HTTPS, and ensure proper configuration of Wi-Fi connections to your business network.

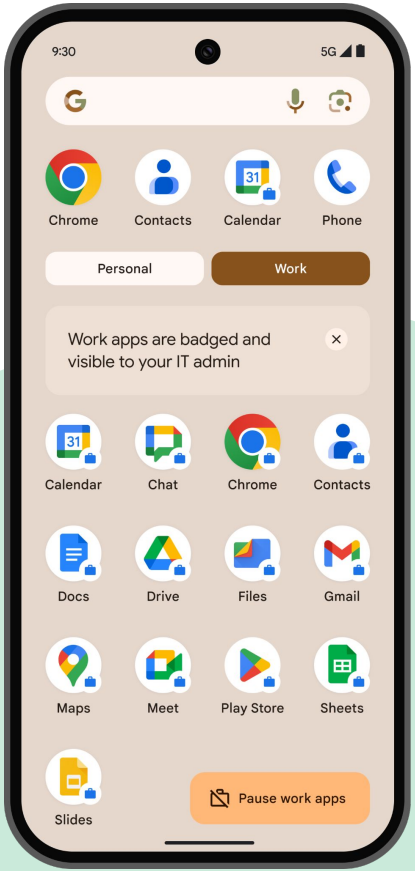
Android's built-in encryption and VPN support helps ensure your data is protected, whether it's stored on the device or transmitted over the network.

08 Utilize Android Work Profile

Best Practice

If employees use personal devices (BYOD), Admins should implement a Work Profile to separate business and personal data on a single device.

The Android Work Profile, an Android only capability, creates a secure walled off environment to help ensure business data is secure and personal data remains private.



Key takeaways

To minimize IT/Help desk calls, it's crucial to train users and offer straightforward guidance on setting up each of the three models.

Refer to the AE Solutions Directory for a selection of approved devices and partners. This resource can assist you in choosing the most suitable products based on your particular requirements.

Prioritize security implementation, even if it's a basic approach. Securing work devices involves costs for each model. Choose a model that balances required security with implementation and maintenance expenses.

Android

Learn more at

www.android.com/enterprise/security