New Management Features in Android

Andy Zmolek

Android Ecosystem Cat Herder and Evangelist

android

The world's most popular **mobility platform**...

2B+
30-day active users

400+
OEMs developing for Android

500+
operator partnerships

1.5M
Android devices activated daily

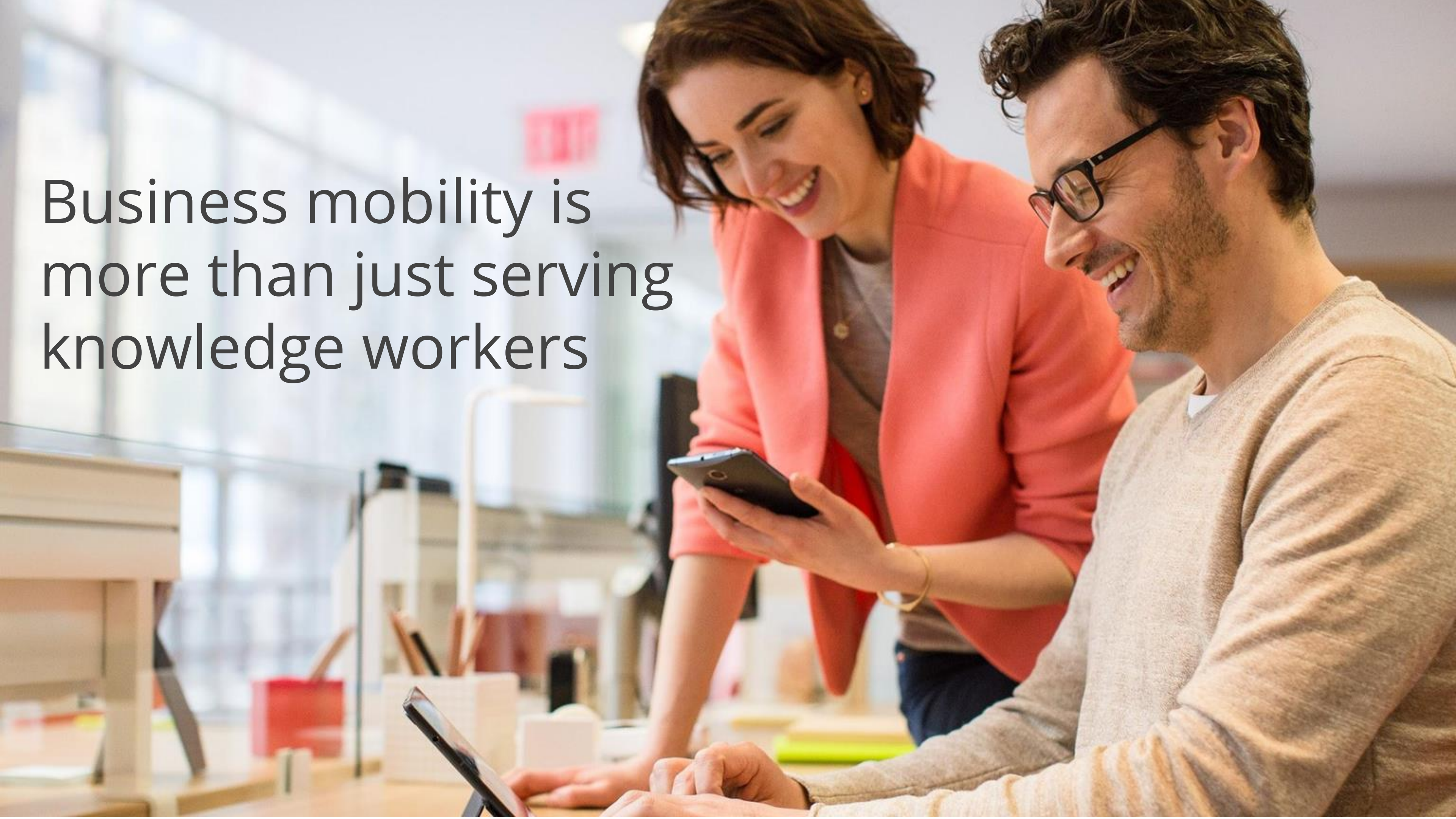
Largest **distribution platform** in the world

65B+
App installs through Play

1M+
Apps available

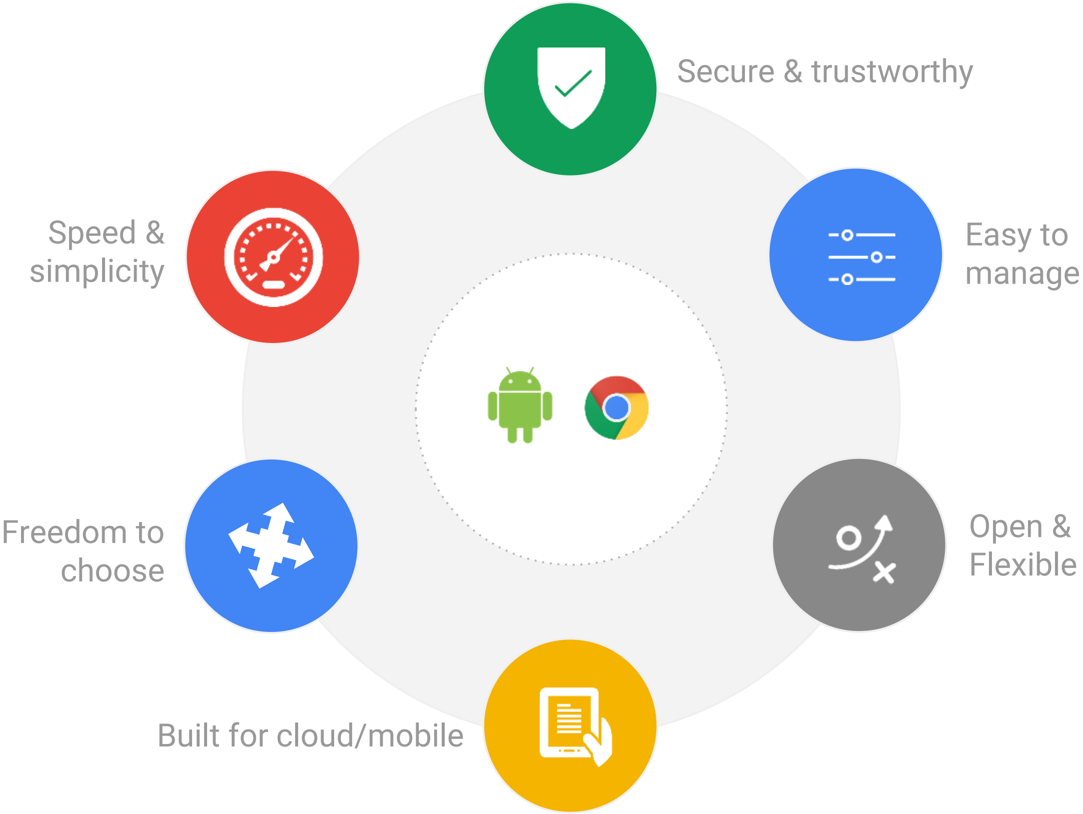
1B+
30-day active users of Google Apps

Business mobility is more than just serving knowledge workers



It’s about transforming the way companies do business

Google vision for devices



Secure & trustworthy

Easy to manage

Open & Flexible

Built for cloud/mobile

Freedom to choose

Speed & simplicity

GOOGLE BELIEVES THAT THE ZEBRA RELATIONSHIP IS:
“KEY TO OUR ENTERPRISE EFFORTS”

Why does this makes sense for Google?

#1

Leader in the Rugged device space

Early Adopter of Android Enterprise

Embrace Android GMS

ZEBRA

WHY IS THIS RELATIONSHIP IMPORTANT?

Purpose Built Devices may represent the greatest growth opportunity across the ecosystem - for OEMs, ISVs, Device Management solutions and Carriers alike

GOOGLE TO SUPPORT MULTIPLE ZEBRA PARTNER EFFORTS

Strategic Accounts Support

Channel Partner Joint events

Presentations at App**Forums**

Development Support (Migration, DevHub)

Get customers excited about future possibilities

Enjoy the ride together!

Management

Lollipop

Separate managed work profile and private user profile for BYOD

Device Owner for corp-liable devices

Marshmallow

Device Owner APIs for COSU

Polish for BYOD

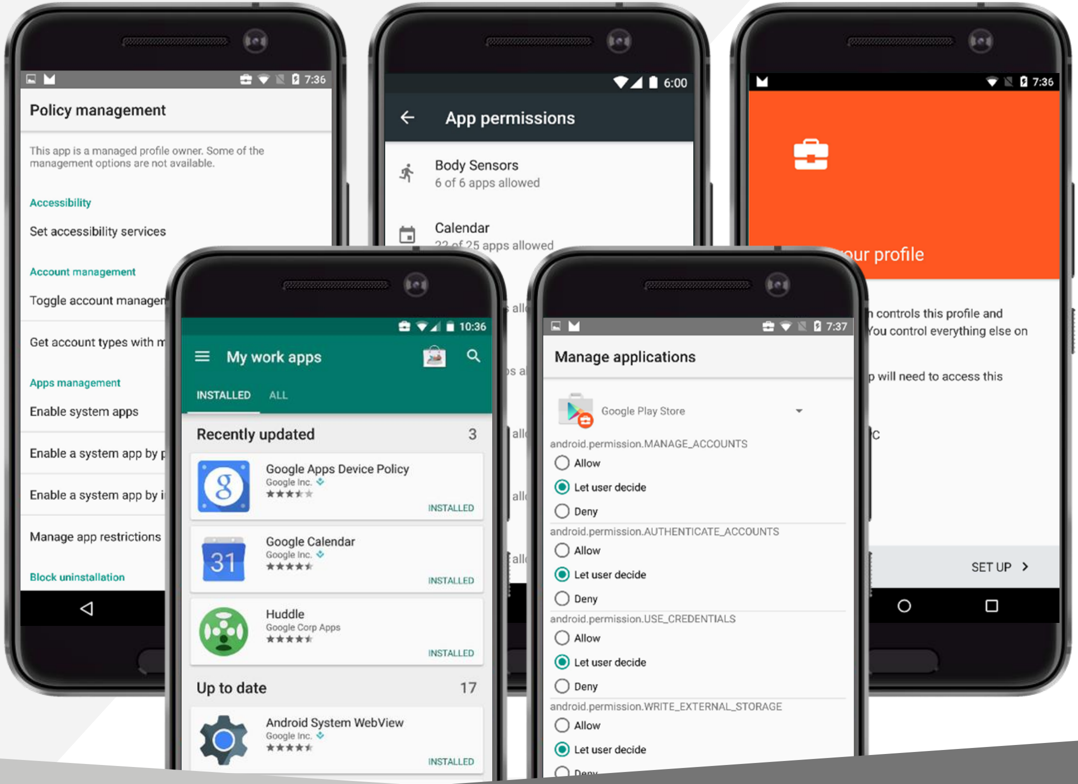
Nougat

Addressed Customer feedback

Boosted security and control for IT admin

Polish and control for the user

Customization and Manageability



7:36

Policy management

This app is a managed profile owner. Some of the management options are not available.

Accessibility

Set accessibility services

Account management

Toggle account managen

Get account types with m

Apps management

Enable system apps

Enable a system app by p

Enable a system app by i

Manage app restrictions

Block uninstallation

6:00

App permissions

Body Sensors
6 of 6 apps allowed

Calendar
22 of 25 apps allowed

7:36

our profile

n controls this profile and
You control everything else on

p will need to access this

SET UP >

10:36

My work apps

INSTALLED ALL

Recently updated 3

Google Apps Device Policy
Google Inc.
INSTALLED

Google Calendar
Google Inc.
INSTALLED

Huddle
Google Corp Apps
INSTALLED

Up to date 17

Android System WebView
Google Inc.
INSTALLED

7:37

Manage applications

Google Play Store

android.permission.MANAGE_ACCOUNTS
○ Allow
● Let user decide
○ Deny

android.permission.AUTHENTICATE_ACCOUNTS
○ Allow
● Let user decide
○ Deny

android.permission.USE_CREDENTIALS
○ Allow
● Let user decide
○ Deny

android.permission.WRITE_EXTERNAL_STORAGE
○ Allow
● Let user decide
○ Deny

Management configurations support BYOD, company owned and purpose-built devices:

- → Work profile can protect and isolate work data from personal data for BYOD solutions.
- → Work Managed Device gives access and control to complete device and can be purpose built to run a specific set of apps.

Variety of purpose-built devices support comprehensive solutions:

- → Diversity of form factors
- → Different price points
- → Rugged devices
- → Workflow devices
- → Signage

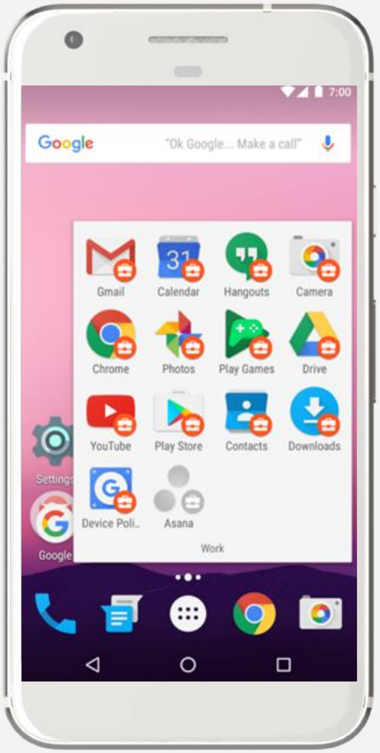
Work Profile

→ **Provide work/life balance:**

- Work profile
- Turn off work mode

→ **Ensure personal privacy:**

- Isolate work data
- Prevent removal of personal assets (photos, contacts, etc.) with selective wipe.



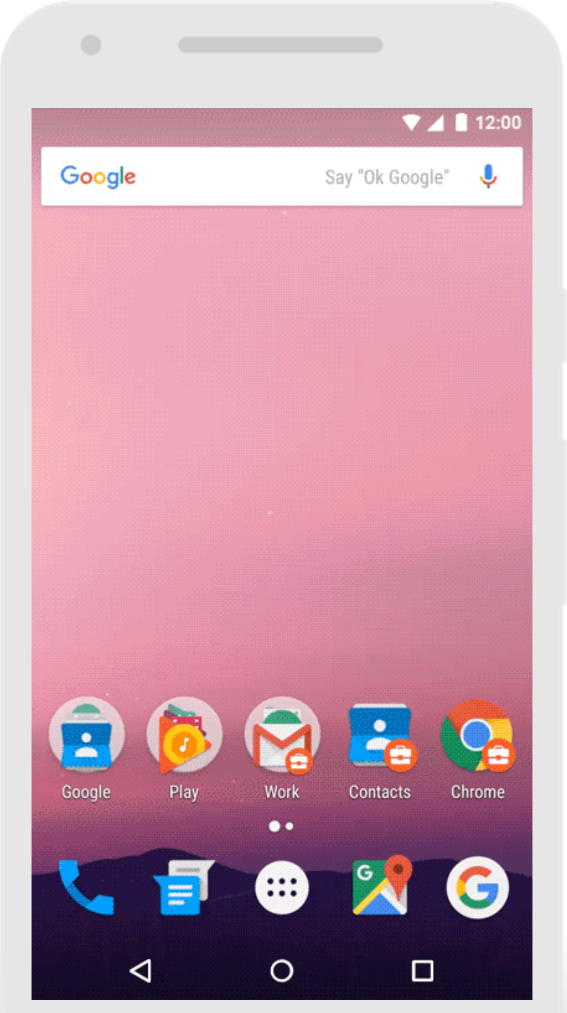
Work Profile

NEW IN 7.0 NOUGAT

User experience highlights

Turn off Work Mode

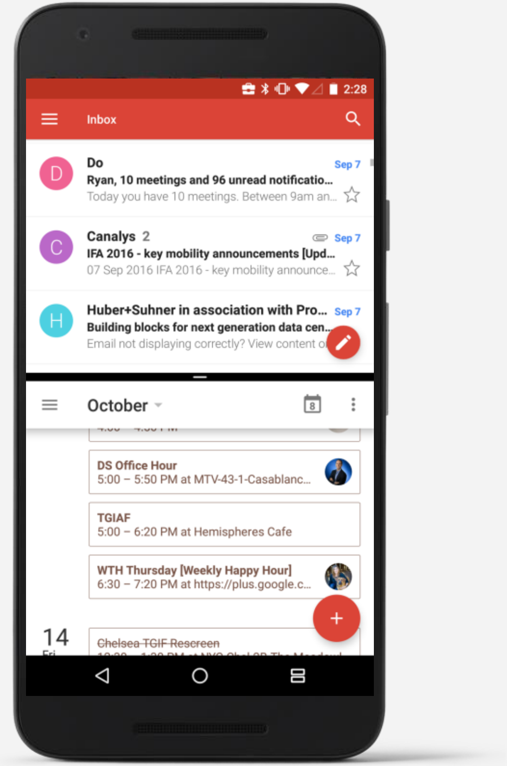
By turning off Work Mode, employees can completely disable their device's Work Profile, including apps, notifications, and background sync so they can set their own work-life boundaries.



Work Managed Device

→ Full device control:

- Set policies on every aspect of the device - bluetooth, wifi,
- Control exactly what applications are deployed to the device, even restricting it to just one
- Wipe the entire device if necessary



D Do Sep 7
Ryan, 10 meetings and 96 unread notificatio...
Today you have 10 meetings. Between 9am an...

C Canalys 2 Sep 7
IFA 2016 - key mobility announcements [Upd...
07 Sep 2016 IFA 2016 - key mobility announce...

H Huber+Suhner in association with Pro... Sep 7
Building blocks for next generation data cen...
Email not displaying correctly? View content o

DS Office Hour
5:00 – 5:50 PM at MTV-43-1-Casablanc...

TGIAF
5:00 – 6:20 PM at Hemispheres Cafe

WTH Thursday [Weekly Happy Hour]
6:30 – 7:20 PM at https://plus.google.c...

14

~~Chelsea TGIF Rescreen~~

Multi-tasking Tools

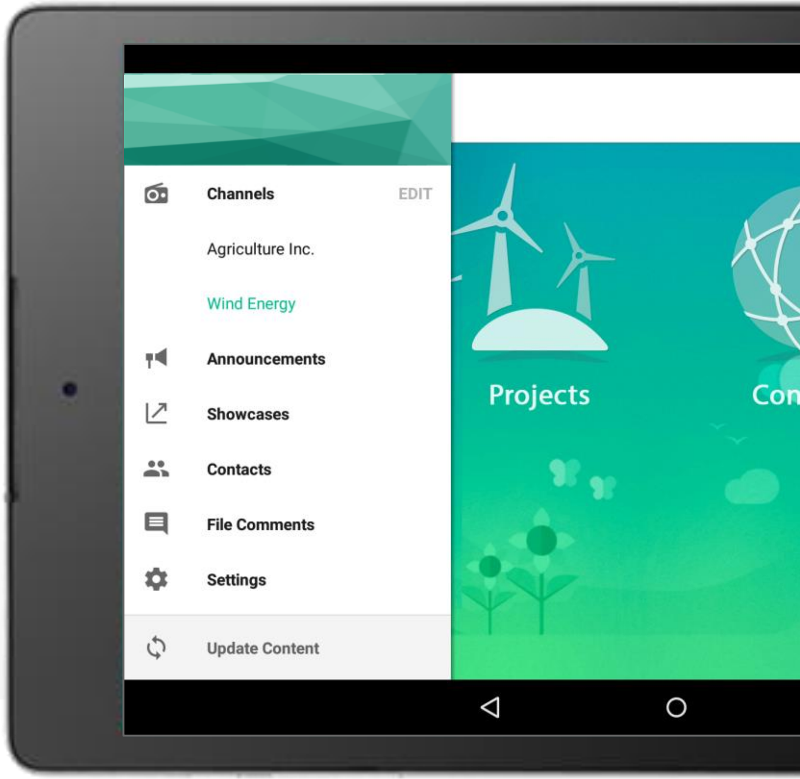
Management highlights

Single use mode for COSU

Locks device down into special mode running single or set of specific apps.

Admins can remotely control settings and app install/uninstall over the air (OTA).

Provisioning device is as simple as a near field communication (NFC) bump.



Simplified Management Controls for the Enterprise

Setup and policy control:

- → **Standardized Controls** enable the same level of policy access on any Android device. And you can set these policies through your EMM vendor.
- → **Management Configurations** such as the Work Profile and Work Managed Device allow control over how data is shared between work and personal applications

Setup and policy control:

- → **Permission Controls** manage access and runtime.
- → **Setup Wizard** supports QR codes, saving significant time in setup.
- → **Temporary Suspend** allows for control of access to work apps based on compliance.

Simplified Management Controls for the Enterprise

r isolated
cies to

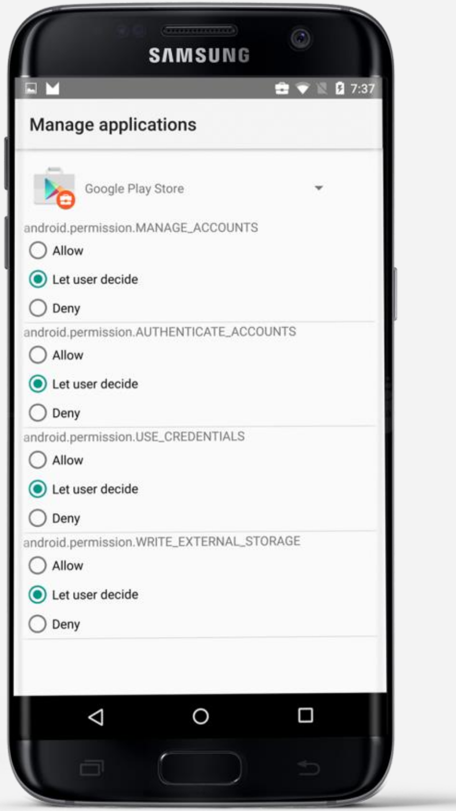
partners
ccount-
nsole

Setup and policy control:

→ **Permission Controls** manage access and runtime at an application

→ **Temporary Suspend** allows for control of access to work apps based on IT policy compliance.

→ **Google Play** enables secure and simplified app distribution, management, and bulk purchasing, including legacy devices.



Manage applications

Google Play Store

android.permission.MANAGE_ACCOUNTS
○ Allow
● Let user decide
○ Deny

android.permission.AUTHENTICATE_ACCOUNTS
○ Allow
● Let user decide
○ Deny

android.permission.USE_CREDENTIALS
○ Allow
● Let user decide
○ Deny

android.permission.WRITE_EXTERNAL_STORAGE
○ Allow
● Let user decide
○ Deny

Permission Controls

android

Simplified Management Controls for the Enterprise

lified app

t devices
nd

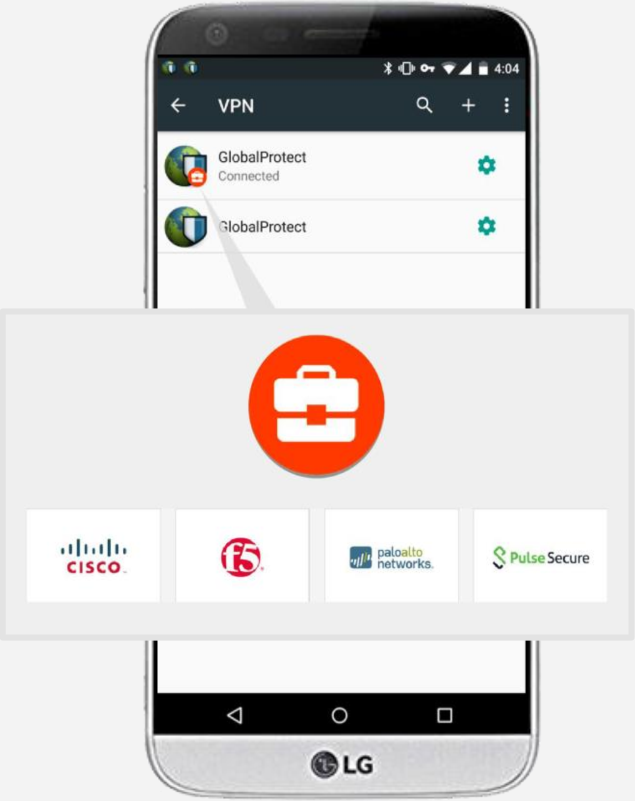
ng and
ess to

Ongoing deployment and scaling:

→ **Logging and Monitoring APIs** allow access to data usage statistics and logging across devices.

→ **VPN and Wifi Settings** control how applications access your network and intranet

→ **Policy Transparency** enables full disclosure of policies and restrictions for increased employee understanding.



VPN Settings

NEW IN 7.0 NOUGAT

Management highlights

Fast and secure set-up

With setup wizard for work now supporting QR code scanning, setting up Work Managed Devices can be significantly faster.

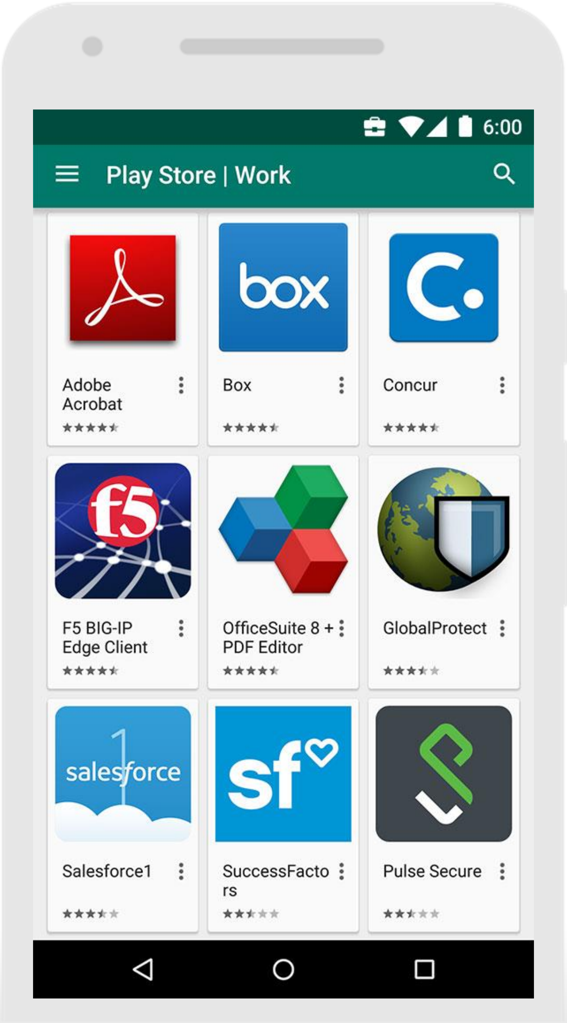
Management highlights

Managed Google Play

Allows IT to securely deploy and manage business apps

Any app in the Play catalog to be deployed to the work profile

Simplifies app distribution and ensures IT approves every app deployed



Managed Play Accounts

No need for Google Accounts
Customer doesn't want employees to have access to other Google services

No need for passwords
Customer doesn't want passwords to sync or manage

No need for separate AD/LDAP Sync
EMM partners generally already do this, puts the identity lifecycle in the hands of the EMM only

No visibility to end user
These accounts are limited and generally hidden from the view of the end user (shows up only inside Account Manager)

Managed Play Accounts put the EMM in charge of creation, management, and deletion

Managed Google Accounts

When full Google Accounts are desired
Customer doesn’t needs employees to have access to other Google services such as G-Suite

Employee accounts must have passwords
Customer can sync passwords but employees need to be able to use Google accounts in other contexts, like web

Direct Customer Control of Identity
Customer wants to directly control identity lifecycle either through sync or other manual or automated means

Visibility to end user
These Google accounts are visible to the end user throughout their Android and web experiences

Managed Google Accounts put the customer in charge of creation, management, and deletion (can also be delegated to their EMM)

Test Drive the Android Management Experience at
enterprise.google.com/android/experience

GMS and Security

Seven products with over **one billion users each**, available through Google Mobile Services

Google Search

Android

Chrome

Google Maps

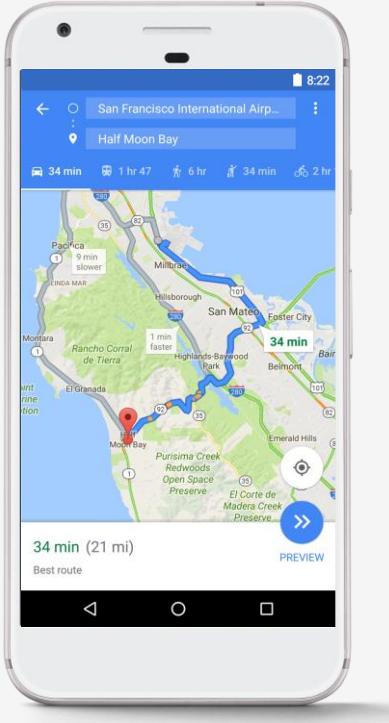
Google Play

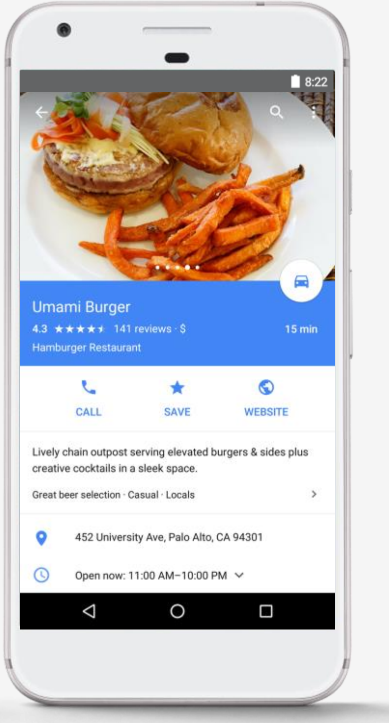
YouTube

Gmail

android

GMS and Geo: Google Maps and Maps APIs



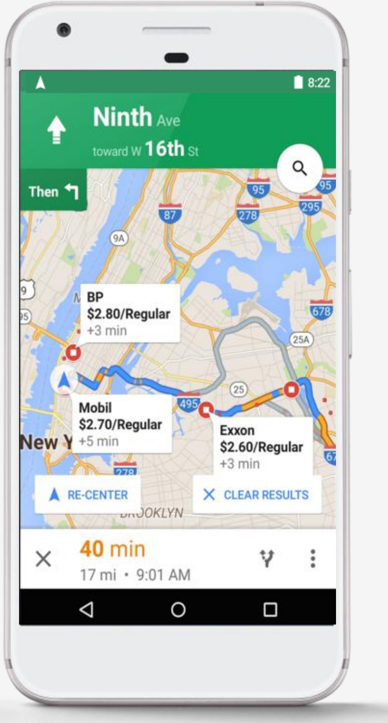


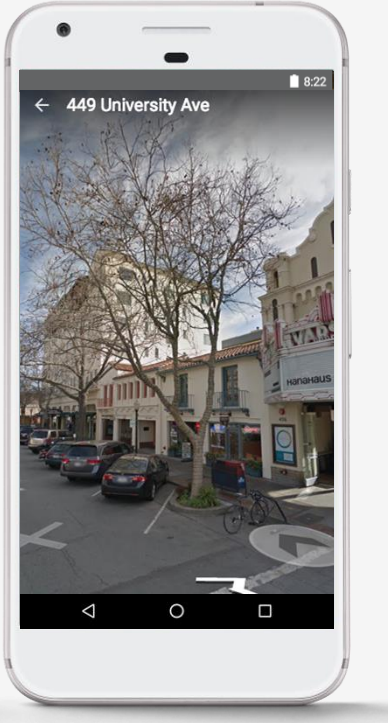
Lively chain outpost serving elevated burgers & sides plus creative cocktails in a sleek space.

Great beer selection · Casual · Locals

452 University Ave, Palo Alto, CA 94301

Open now: 11:00 AM–10:00 PM





Google Play

Protect

Security protections for Android and Play, for everyone.

Built into every device with Google Play. Always updating to provide the latest protections by Google.

2 billion

devices protected

1+ billion

device scans per day

50+ billion

apps checked per day

App analysis at scale

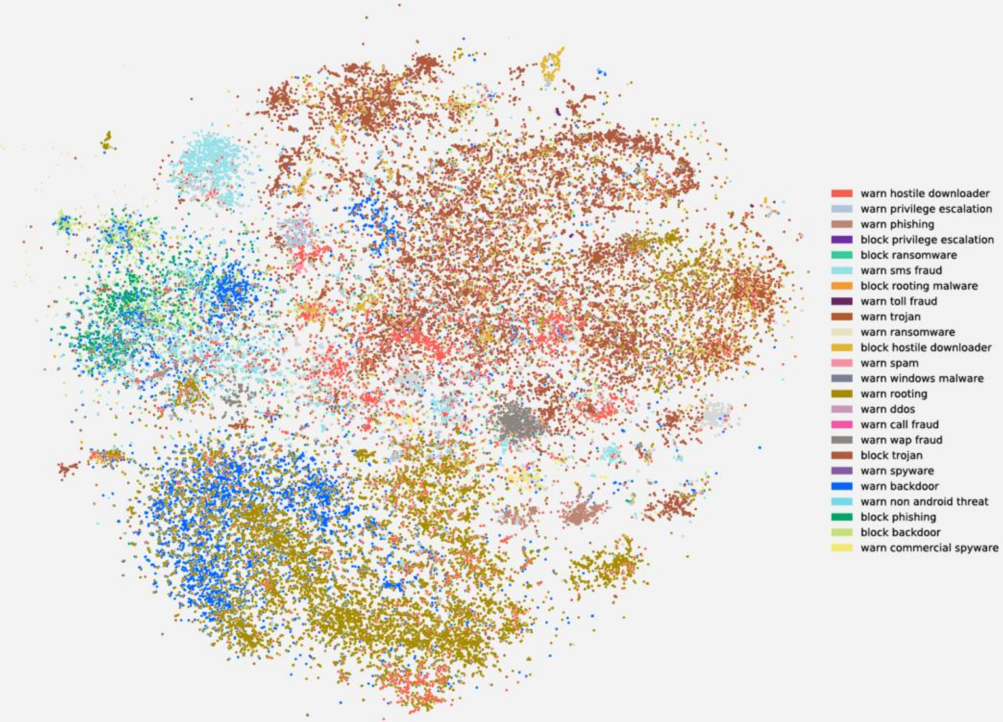
20k dedicated processors, 24/7

500k+ apps analyzed daily

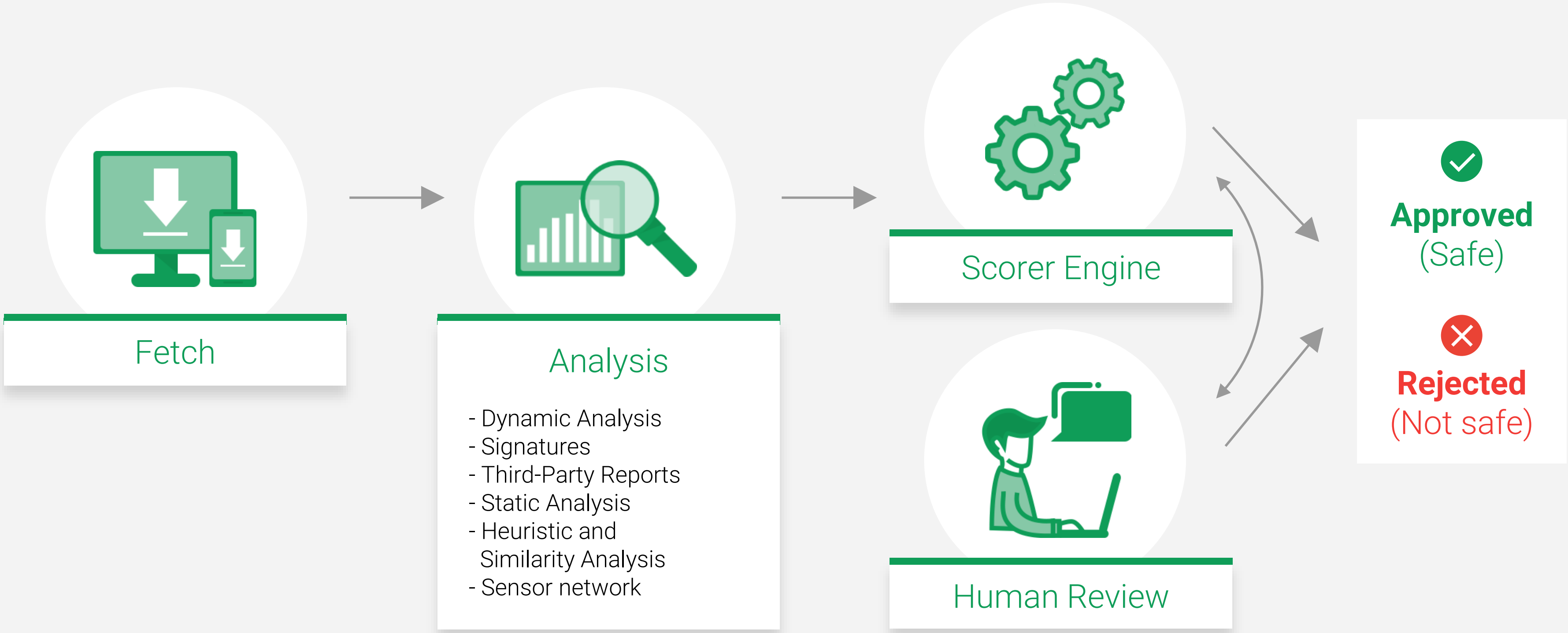
Machine Learning

Google employs machine learning techniques and statistical analysis to pinpoint potentially harmful apps.

Billions of data points a day help our systems learn to spot unusual behavior and anomalous patterns.



Applications review process



Fetch

Analysis

- Dynamic Analysis
- Signatures
- Third-Party Reports
- Static Analysis
- Heuristic and Similarity Analysis
- Sensor network

Scorer Engine

Human Review

✓ **Approved** (Safe)

✕ **Rejected** (Not safe)

How does it work?

Static analysis

Extracting features from app code

Dynamic analysis

App is run in our emulated Android environment

Sensor network

Feedback of app behavior from every device

Similarity analysis

Comparison of apps with others that have similar properties

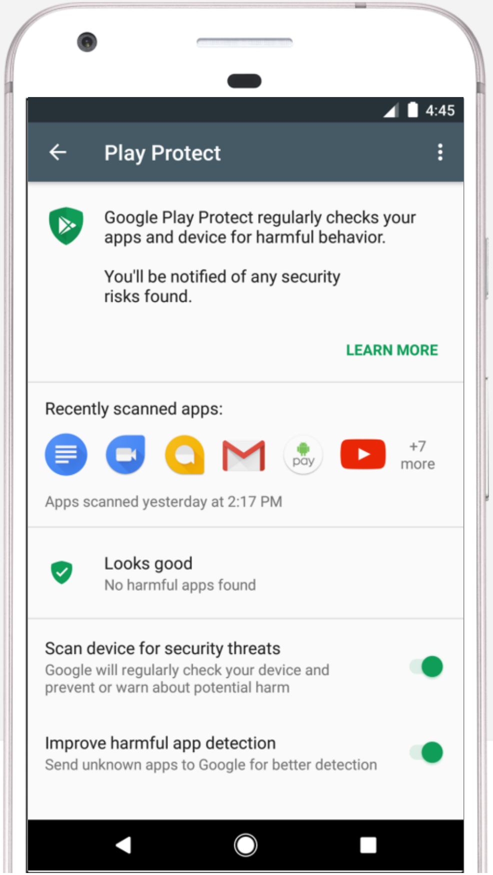
Developer relationships

Play developer info & app certificated used to associate apps

Third-party reports

Active collaboration with researchers and security professionals

Transparency across Android and Play



Play Protect

Google Play Protect regularly checks your apps and device for harmful behavior.

You'll be notified of any security risks found.

LEARN MORE

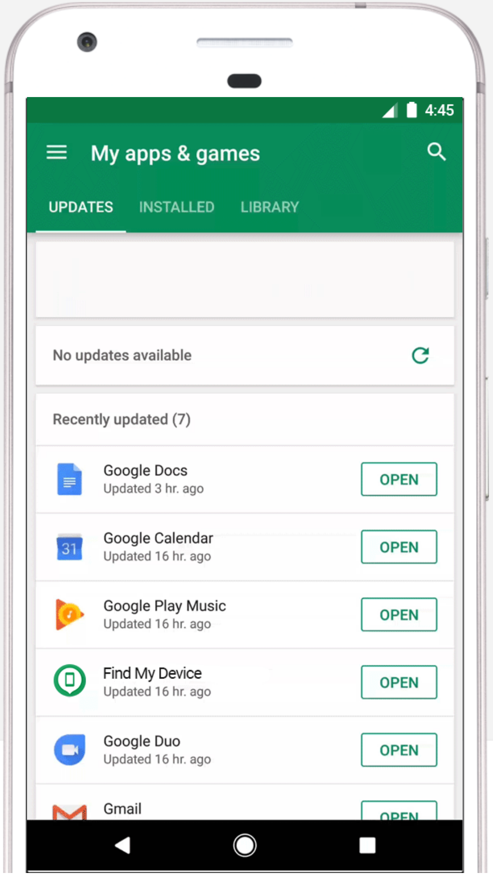
Recently scanned apps:

Apps scanned yesterday at 2:17 PM

Looks good
No harmful apps found

Scan device for security threats
Google will regularly check your device and prevent or warn about potential harm

Improve harmful app detection
Send unknown apps to Google for better detection



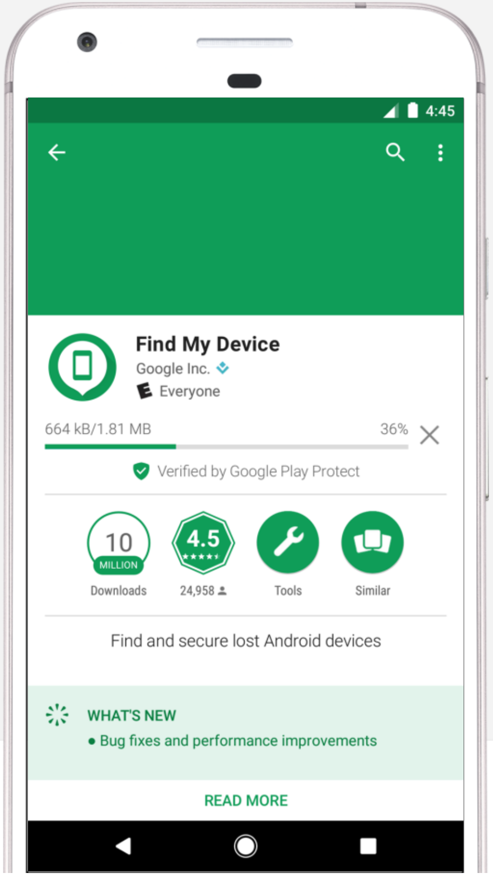
My apps & games

UPDATES INSTALLED LIBRARY

No updates available

Recently updated (7)

Google Docs Updated 3 hr. ago	OPEN
Google Calendar Updated 16 hr. ago	OPEN
Google Play Music Updated 16 hr. ago	OPEN
Find My Device Updated 16 hr. ago	OPEN
Google Duo Updated 16 hr. ago	OPEN
Gmail	OPEN



Find My Device
Google Inc.
Everyone

664 kB/1.81 MB 36%

Verified by Google Play Protect

Find and secure lost Android devices

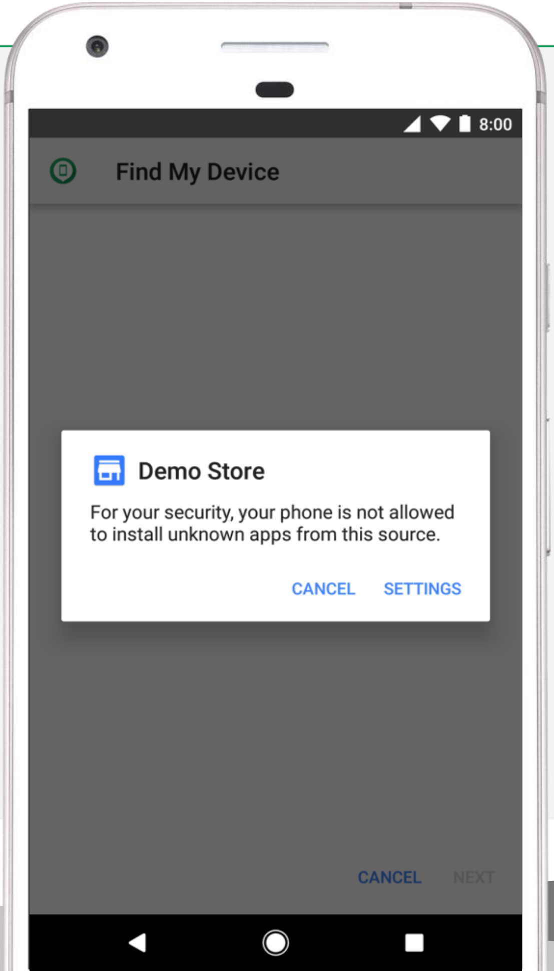
WHAT'S NEW
- Bug fixes and performance improvements

READ MORE

Installing Unknown Apps

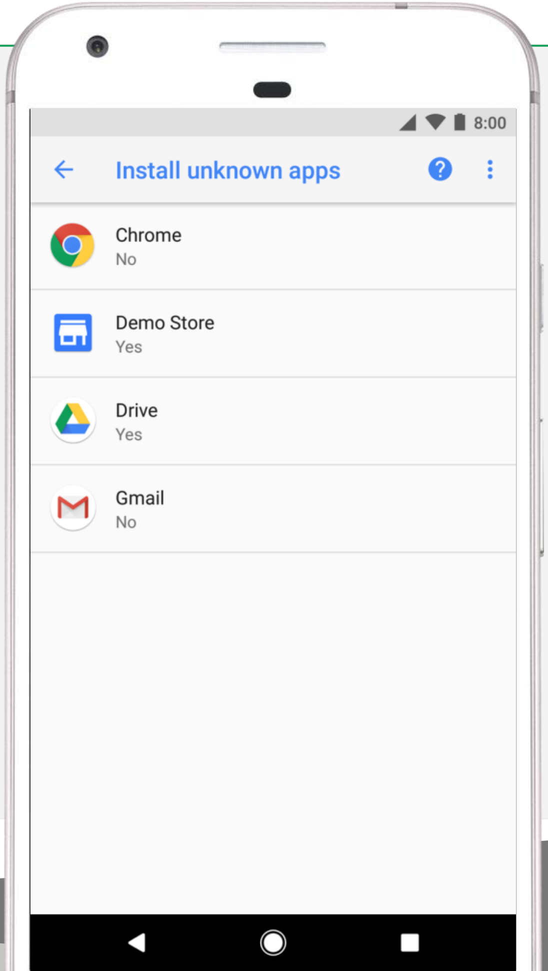
Finer-grained control for allowing app installs, reducing threat from hostile downloaders.

“Unknown sources” switch is now a per-install-source permission in Android O.



Demo Store

For your security, your phone is not allowed to install unknown apps from this source.



Install unknown apps

Chrome
No

Demo Store
Yes

Drive
Yes

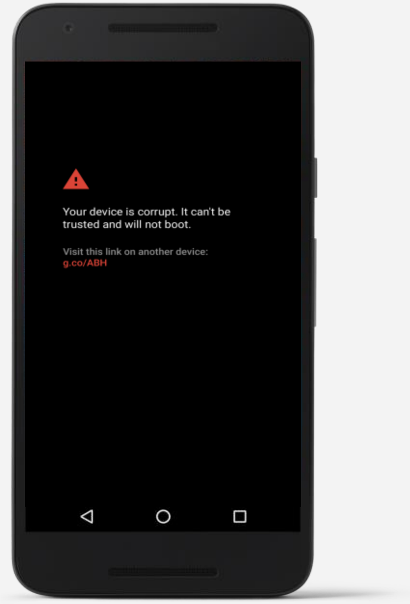
Gmail
No

Verified Boot

Verification required for compatible devices

Strictly enforced for compatible devices

Guidance for:
1. Rollback protection
2. Hardened unlocking



Your device is corrupt. It can't be trusted and will not boot.

Visit this link on another device:
g.co/ABH

Encryption

Must be enabled for compatible devices

File-based encryption (FBE) recommended

FBE enhancements: key ejection, etc.

7:00
TUESDAY, 16 AUGUST
Unlock for all features and data
Unlock for all features and data

Secure Lock screen

Fingerprint support backed by secure hardware (e.g. TEE)

PIN verification in secure hardware

Tamper-resistant hardware support (e.g. SE)

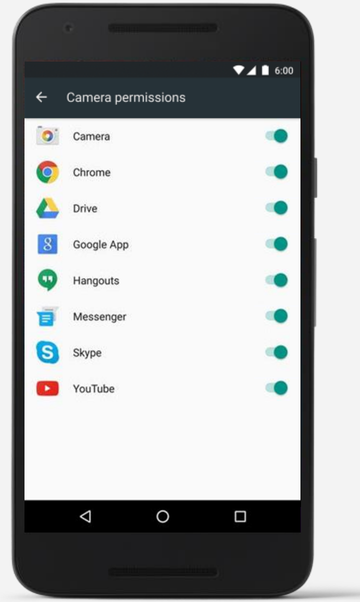
Permissions

Runtime permissions

Descoping device admin API

Updated overlay API

Removed access to most persistent IDs



6:00

Camera permissions

- Camera ●
- Chrome ●
- Drive ●
- Google App ●
- Hangouts ●
- Messenger ●
- Skype ●
- YouTube ●

Webview Security

Shipped with the operating system

Separate APK updateable via the Play store

Renderer in isolated process

Safe Browsing

Other resources

Youtube - Google Cloud Channel

Google Security Services for Android : Mobile Protections at Google Scale (Google Cloud Next '17)

Youtube - Android Developers Channel

What's New in Android Security (Google I/O '17)

android

Thank you

zmolek@google.com

🐦 @zmolek