android

Android Enterprise

Every worker. Every use case.

Powering the next wave of enterprise mobility

Android enables organizations to use the right mobile devices and solutions for every job, to empower employees to work smarter and open up new business possibilities, all with the security and control you need.

android

2

Enterprise mobility needs to catch up with enterprise reality.

It's never been more important to get mobility right. Enterprises today use more mobile endpoints than ever to handle more critical tasks. They face ever-higher stakes for security and compliance, and the rapidly growing need to support a distributed global workforce.

Despite this, most enterprises are far from realizing the full potential of mobility. Large percentages of mobile devices go unmanaged. Large portions of the workforce have no mobile access. Security vulnerabilities and gaps in admin capabilities persist.
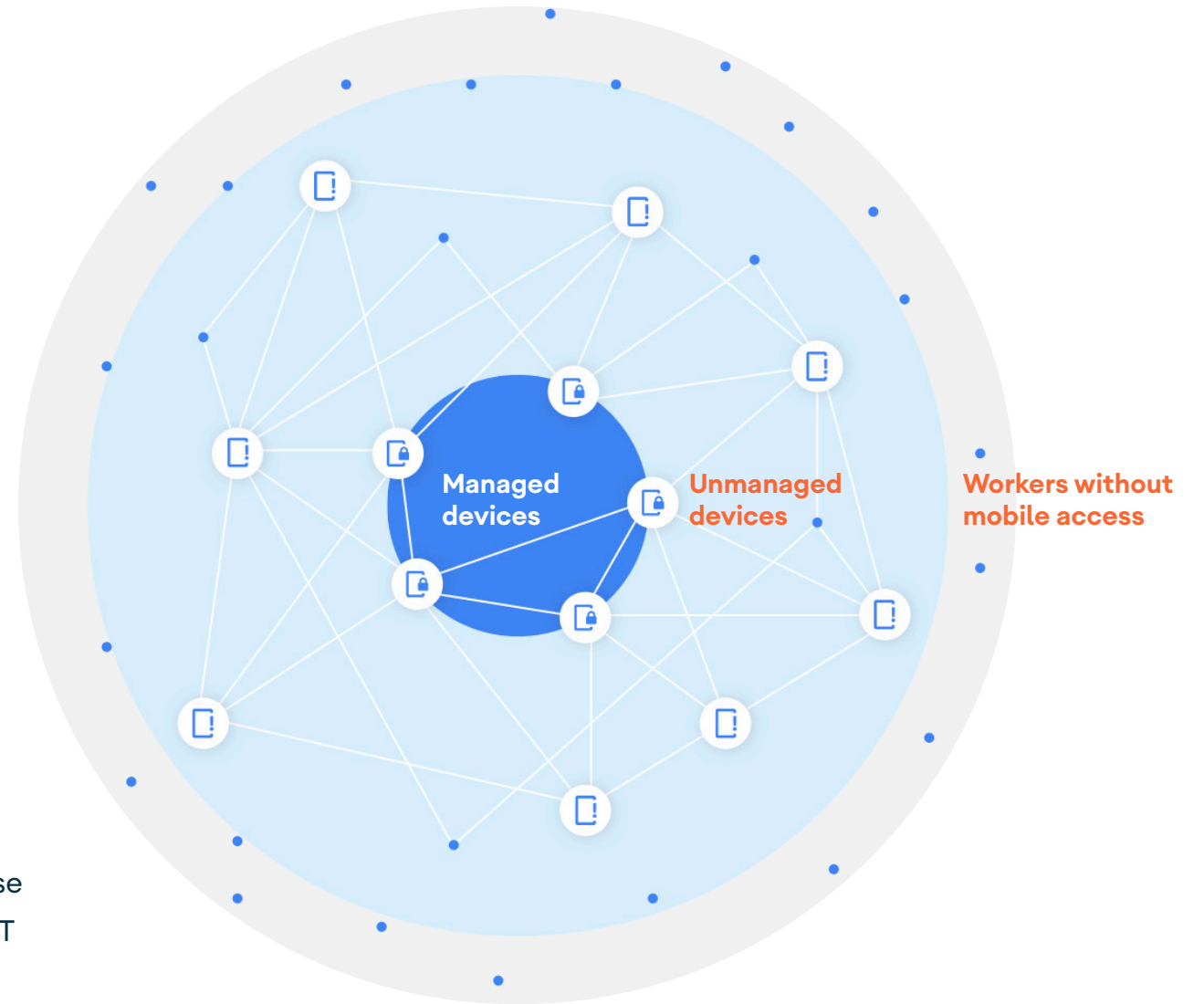
Recent research studies have shown:

70%
of end-users expect to be productive from anywhere[1]

47%
of ITDMs say they don't have a clear BYOD security policy[2]

39%
of companies experienced a security compromise involving mobile/IoT devices during the past year[3]

Managed devices

Unmanaged devices

Workers without mobile access

android

Empower every worker. Support every use case.

Android is already the world's most popular mobile platform, with over two billion active users and a rapidly growing presence in the enterprise. Today, 78% percent of business devices in use worldwide are running Android, according to IDC.[4]

Only Android offers a range of devices capable of connecting every worker—from the boardroom to the factory floor. Since the launch of Android 5.0 in 2015, the platform has featured a streamlined management framework that gives enterprises unmatched flexibility and increased security and control.

Android Enterprise provides management APIs for a vast array of use cases, an OS-based approach to data separation on mixed-use devices, and a cutting-edge system for app deployment via managed Google Play.

Android Enterprise never stops innovating, releasing security upgrades and feature enhancements in a continuous cycle, with a constant stream of new capabilities supported by a growing partner ecosystem.

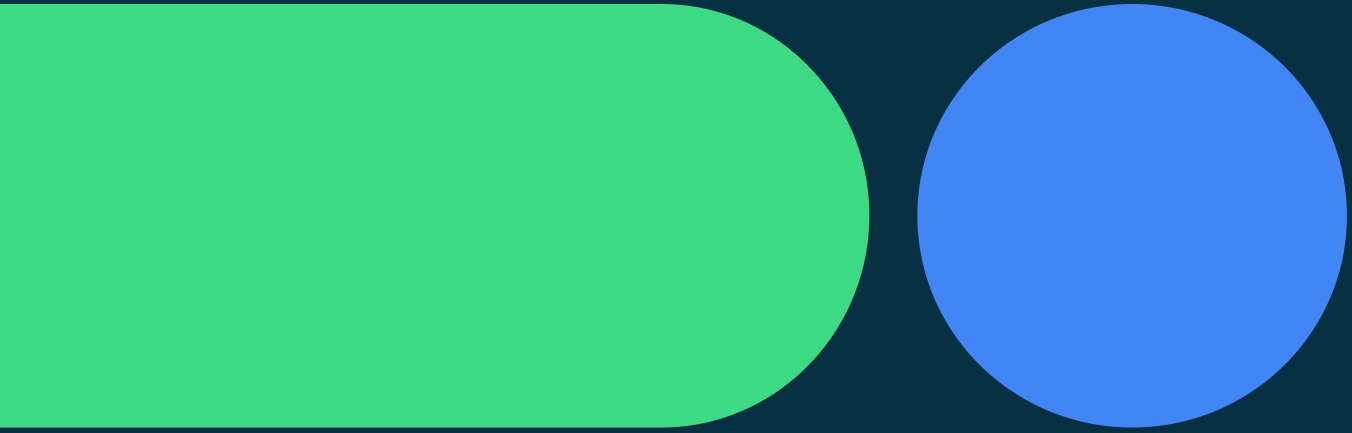Built-in security, backed by Google machine learning

Robust enterprise devices & app management

Applications for every use case

Thousands of device types, fit for purpose

Redefining standards for mobile security

Superior data protection with Android

The success of any mobile deployment hinges on security. And securing mobile endpoints is still a major challenge for any enterprise. According to research conducted by Verizon in 2019, 33% of companies have experienced a compromise due to mobile security risks.[5]

Let's take a look at how Android protects your business, so you can plan, implement, and grow with confidence.

Security challenges

- Data loss
- Unauthorized access
- Compliance with corporate policies
- Lost or stolen devices
- Regulatory compliance

android

Multi-layered security

Android Enterprise solutions are designed with multi-layered security for best-in-class protection right out of the box. Let's look at all the ways Android has evolved to keep your data safe:

Hardware-backed security

Working closely with device manufacturers, Google requires Android Enterprise devices have built-in hardware-backed security — so you can trust devices right out of the box. Once up and running and in the field, hardware-backed security performs critical tasks such as cryptographic operations, authentication and key management. This isolated environment protects private keys and prevents tampering such as brute-force attacks of screen lock PINs and passwords. In fact, hardware-backed security prevents access to these critical services and keys even on a rooted device.

Hardened OS platform

Earning Gartner's highest rating of "Strong" in 26 out of 30 categories, Android delivers best-in-class OS platform security, ensuring device and data integrity.[6] Verified Boot confirms all stages of each device's bootup process, while root detection and kernel protection prevent exploits. Google delivers Android to the ecosystem with FIPS 140-2 validated AES encryption. This encryption is always on and cannot be disabled by users. In addition, sandboxing ensures that every app is isolated and can only access data within its own sandbox.

android

Built-in anti-malware

With Google Play Protect, your team has strong safeguards against the latest malware threats. It's always on and scanning for harmful apps, analyzing apps via the cloud, and using machine learning for protection that gets smarter every day. Real-time malware detection blocks malicious apps from being installed and can alert EMM providers if a threat is detected. Google Play Protect is trusted on over 2.5 billion devices, and scans 100 billion + apps every day.[7] For Android Enterprise managed devices that use Google Play for app distribution, just 0.0004% had a potentially harmful app installed.[7]

Management APIs

Management APIs that streamline the enforcement of any IT security policy, making compliance and data protection easy to manage. For example, SafetyNet—an Attestation API available to the entire Android Enterprise partner ecosystem—provides strong capabilities for testing and determining a device's integrity. APIs like this are available at both the developer and EMM level.
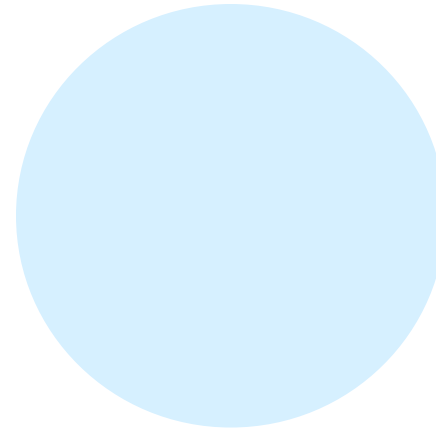
Compliance approved

Android Enterprise meets the strictest privacy and security requirements to comply with Information Security Management Systems, making it ideal across industries — even in regulated spaces like financial services. With SOC 2 and 3 reports, and an ISO 27001 certification, it's in line with the highest security benchmarks and is committed to complying with GDPR.

Managed Google Play gives your IT team the power to securely distribute — and even remotely configure — private and public apps in accordance with best practices and requirements.
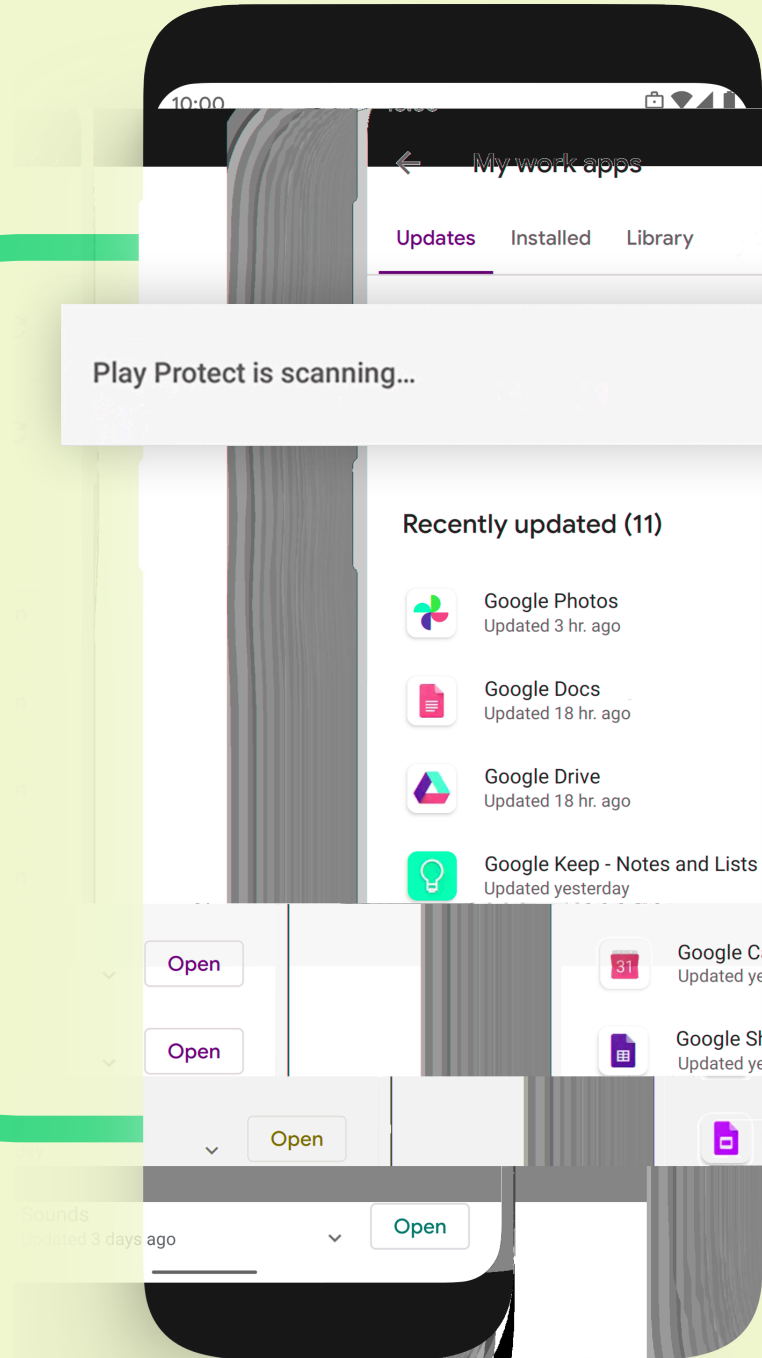
Always up to date

Android provides regular security updates every 30 days, including enterprise grade options that put control back in the hands of IT by allowing you to decide how and when updates happen. This cycle can also be supplemented by as-needed modular updates through Google Play System Updates. This function of Google Play sends the latest security and privacy updates directly to users as they become available.
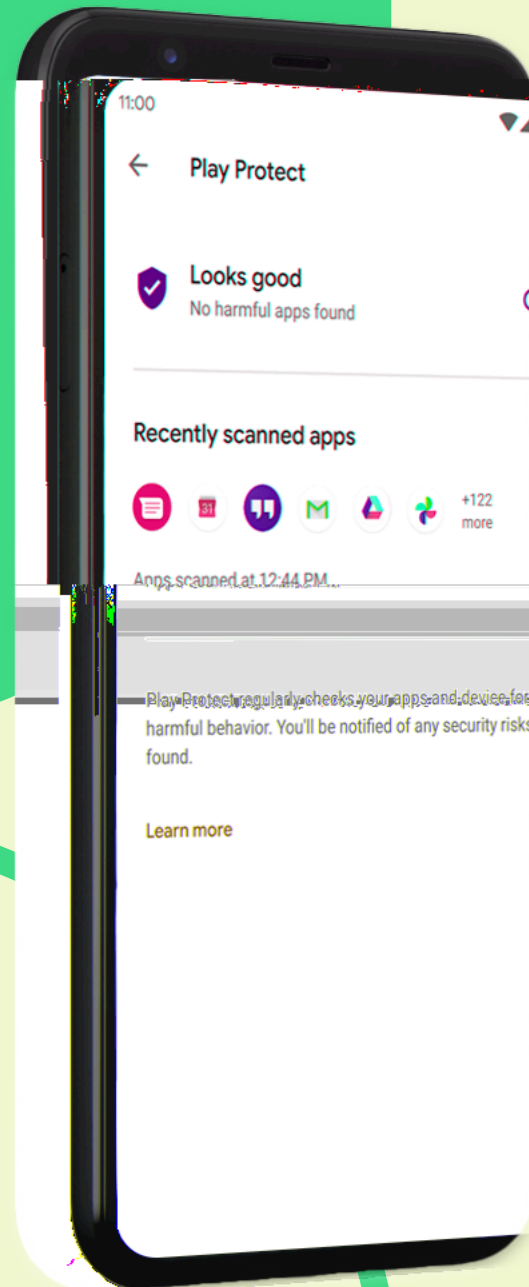
android

Security success

Google Play Protect

Whether it's in your office or out in the field, every Android Enterprise device ships with Google Play Protect, the world's largest mobile threat protection service. And when it comes to success in corporate security, numbers speak louder than words ...

Google Play
Protect

Play Protect is scanning...

Recently updated (11)

Google Photos
Updated 3 hr. ago

Google Docs
Updated 18 hr. ago

Google Drive
Updated 18 hr. ago

Google Keep - Notes and Lists
Updated yesterday

android

Google Play Protect by the numbers
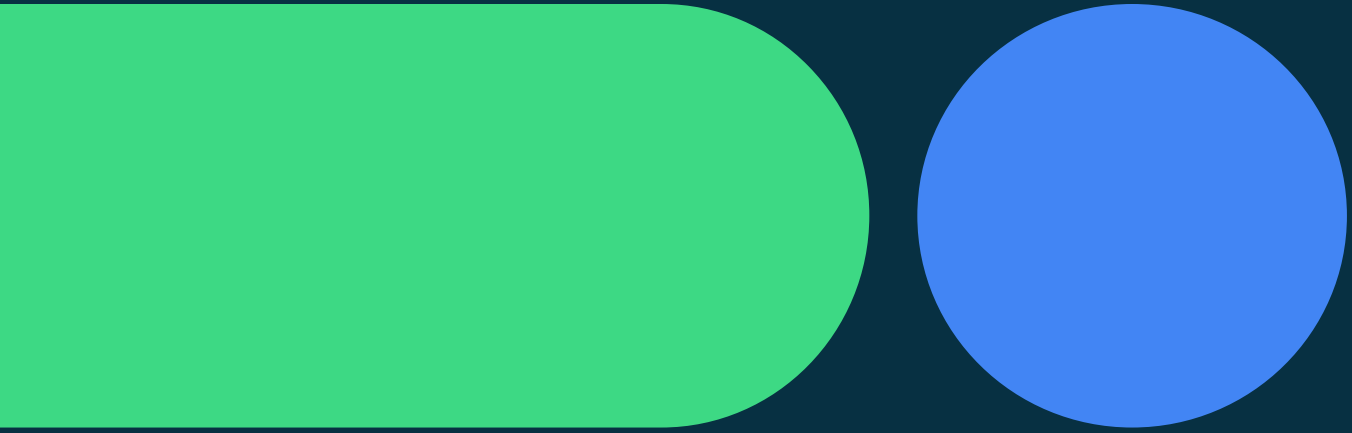

2.5 billion
active devices protected

100 billion+
apps scanned every day

500,000
apps analyzed every day

0.004%
installation of potentially harmful apps on Android Enterprise managed devices that use Google Play for app administration[6]
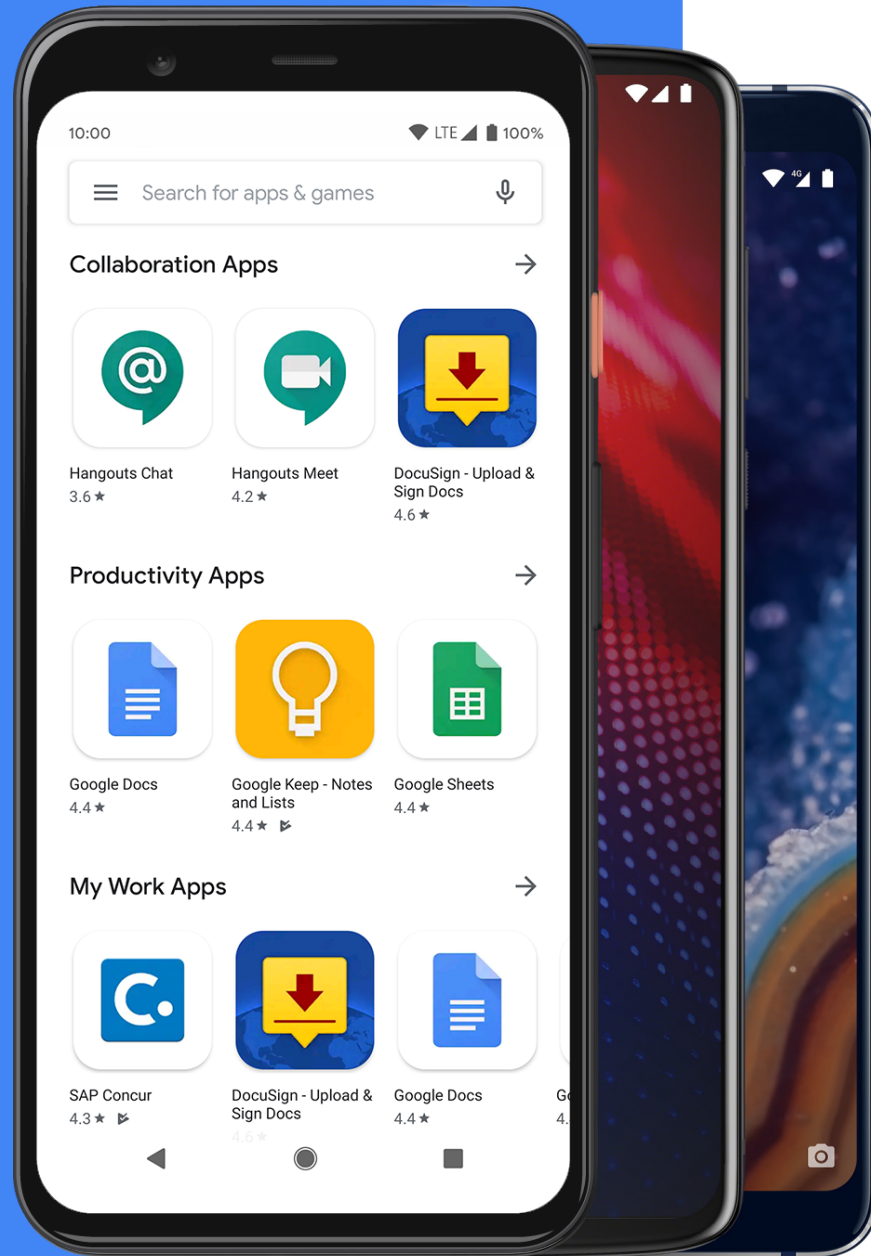
android

Comprehensive and consistent management

Simple and powerful control for IT

As more business is run through the cloud and mobile devices, it's vital to maintain device management in a seamless way that doesn't hinder your employees. You might be worried that this gets more complicated with more devices and types, but Android simplifies management.

Designed for ease of control, Android Enterprise empowers IT with device management that's consistent, powerful, and simple.

Simplified enrollment at scale

Android Enterprise is fleet management made simple. Bulk enrollment tools like zero-touch enrollment, QR code technology, and NFC and DPC identifiers make it easy to configure at scale with both security and consistency in mind.

Zero-touch enrollment

Onboarding with zero-touch enrollment means instant device deployment for your entire fleet — even across multiple brands — with all the apps, configurations, and built-in security you and your employees need right out of the box. It's simplicity for both IT and employees no matter how big, small, local, or global your team is.

Centralized administration

With Android, your EMM console is a powerful hub for comprehensive, centralized management. Everything from creating security policies to creating managed Google Accounts to vetting, whitelisting, and configuring apps — and even publishing in-house apps — can all be done from one interface.

android

Consistent management framework

Android Enterprise provides a consistent set of management capabilities across all Android devices, allowing you to manage devices with ease and efficiency. Android provides built-in management APIs that give the EMM providers options to develop tools that are as varied as they are familiar and reliable. When it comes to enterprise mobility, you'll be ready for any management scenario, including both BYOD and fully managed devices.

Policy and update customization

With Android, employees can create work and personal profiles to keep apps and data separate, and you can set custom data loss prevention policies and control what information can be shared across profiles. You'll have the flexibility to delay over-the-air updates, in order to give your organization more time to test updates from OEMs and carriers, or even choose to update manually offline.
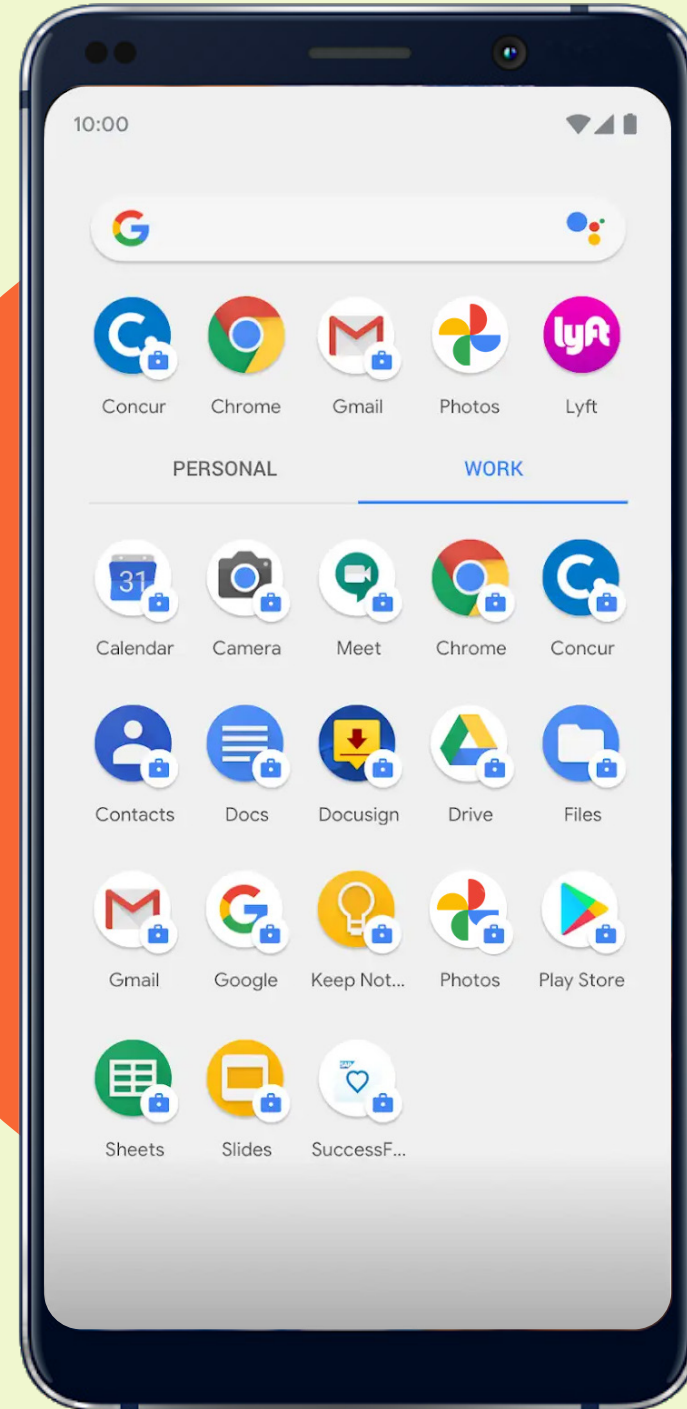
Google verified

With the Android Enterprise Recommended Program, your IT team can make decisions with confidence. Choose from an array of devices and services, which all have been Google verified to meet the most robust requirements for enterprise-ready quality. Google provides regular validation checks on all existing devices and services, and provides standardized support and training through our partner ecosystem, so your team can manage with confidence.
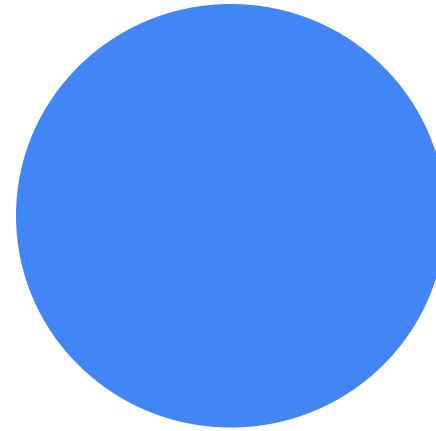
android 🤖

Mobility policies

Android for all

Seamlessly manage your entire fleet and deliver the right mobile experience to the right users. No matter your business's mobility policy, there's an Android Enterprise solution to meet your needs. In fact, Android's comprehensive approach might open up device and service solutions that you'd never thought would be an option for your business.

Personally enabled

Some policies call for company-owned devices that allow personal use. With Android Enterprise, personally enabled devices managed by IT but still can have the same employee privacy protection described for the BYOD policy.*

Work only

In this case, an employee is issued a company-owned device which is not to be used for personal reasons. Android Enterprise empowers IT to fully manage a broad range of device settings and additional policy controls, providing similar management capabilities to personally enabled devices but without privacy-preserving features.

BYOD

A BYOD program offers the promise of cost savings to enterprises, but IT still needs to build a solution that protects the company's interests while preserving user privacy. Android's work profile is a unique, modern approach that separates work and personal apps, data, and policies to protect your business while preserving user privacy. While the user maintains total control and privacy on personal apps and device functions, IT can seamlessly manage work settings, policies, and apps from the managed Google Play store that is customized to fit your specific enterprise needs.

Dedicated device

Sometimes, company-owned devices are dedicated to one task or a small range of tasks. This can be true of devices used in the field, for inventory management, digital signage, ticket printing, or a variety of other tasks. In these cases, IT maintains full control of device settings. They can lock the device to certain apps or use cases, preventing users from enabling unapproved apps or functions.

*Android 11

android

Tested and trusted

Android Enterprise Recommended

When you see the Android Enterprise Recommended badge, you can trust that Google has vetted that product or service to ensure enterprise-grade features and expertise, best-in-class security, and ease of management. So you can master your business's mobility challenges with confidence, no matter how great or small.

8:16
Tuesday, April 6

9:00
THURSDAY, AUGUST 31

12:50 PM

android
enterprise
recommended

Play Store

android
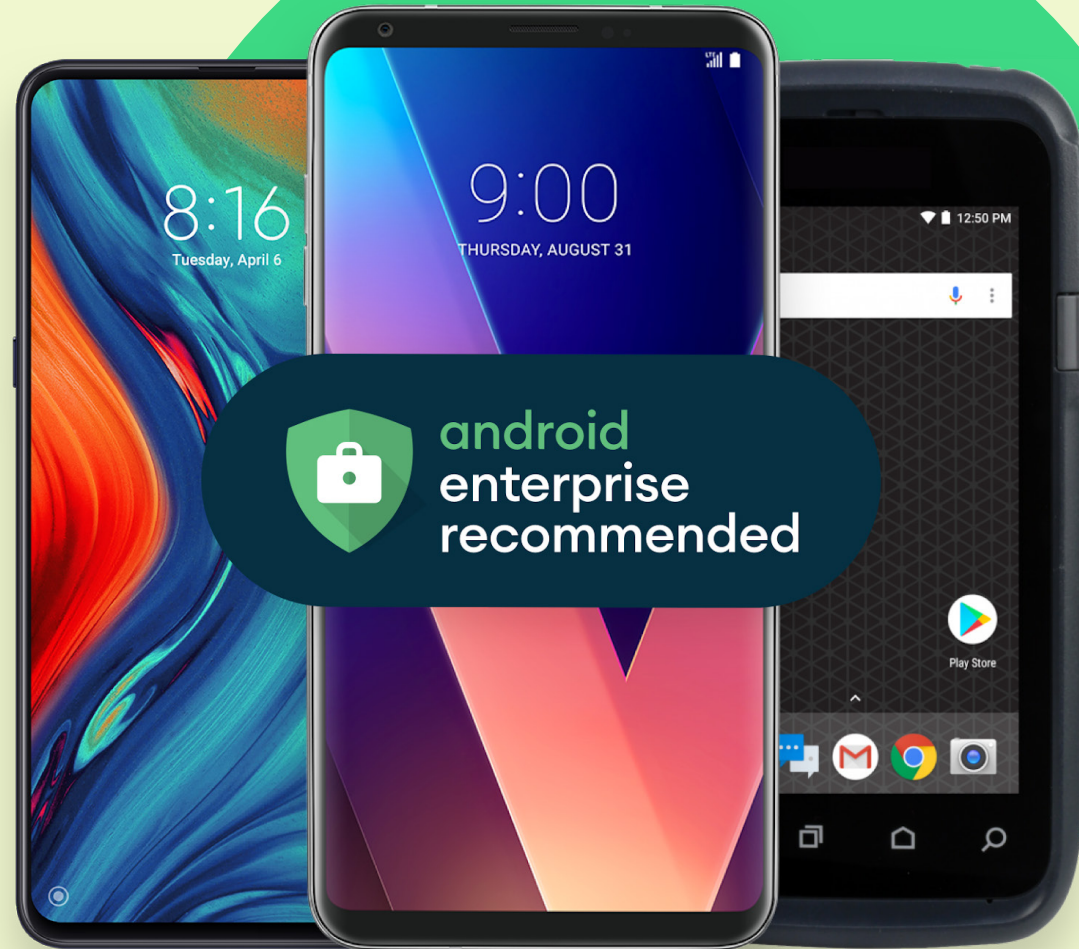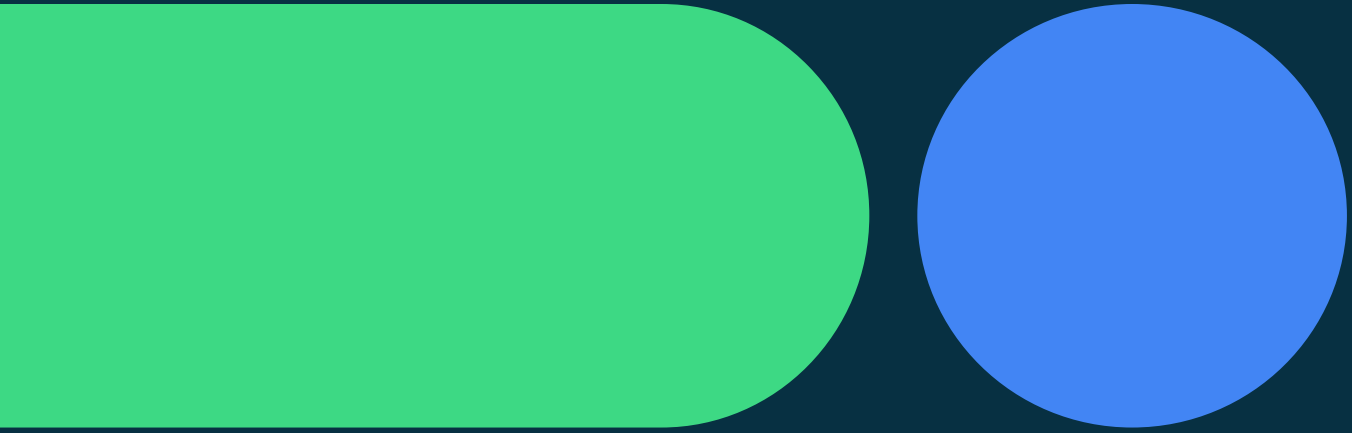
Mobility that empowers your team

Privacy, trust, and balance for employees

Today, over 80% of employees are expressing a desire to work from home at least some of the time.[8] This shift isn't just about where work gets done, it's also about digital well-being. Employees expect mobile tools that keep them productive anywhere while also separating work time from personal time. Privacy is also a concern, as 71% of employees expect personal information on work devices to remain private.[1] Android Enterprise has evolved to meet these expectations, with features that give employees the confidence and flexibility they need to work smarter while striking a healthy work-life balance.
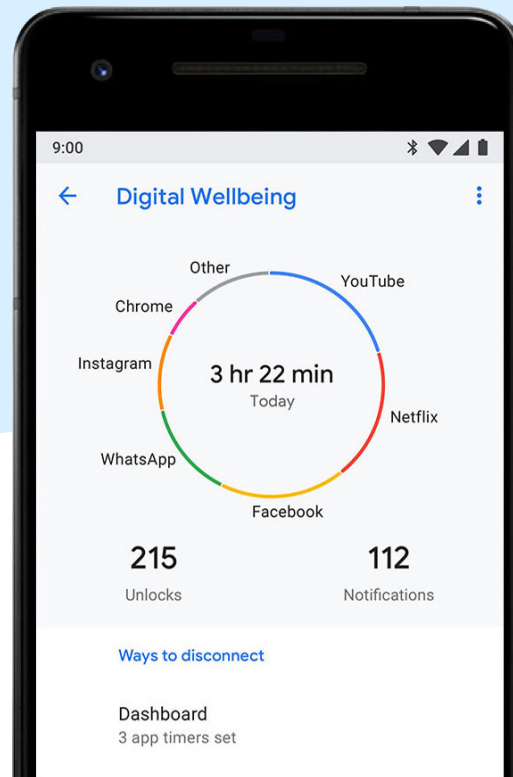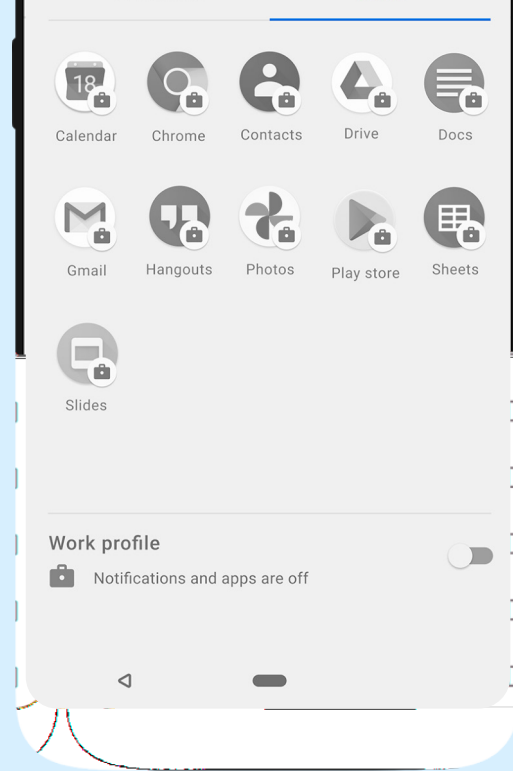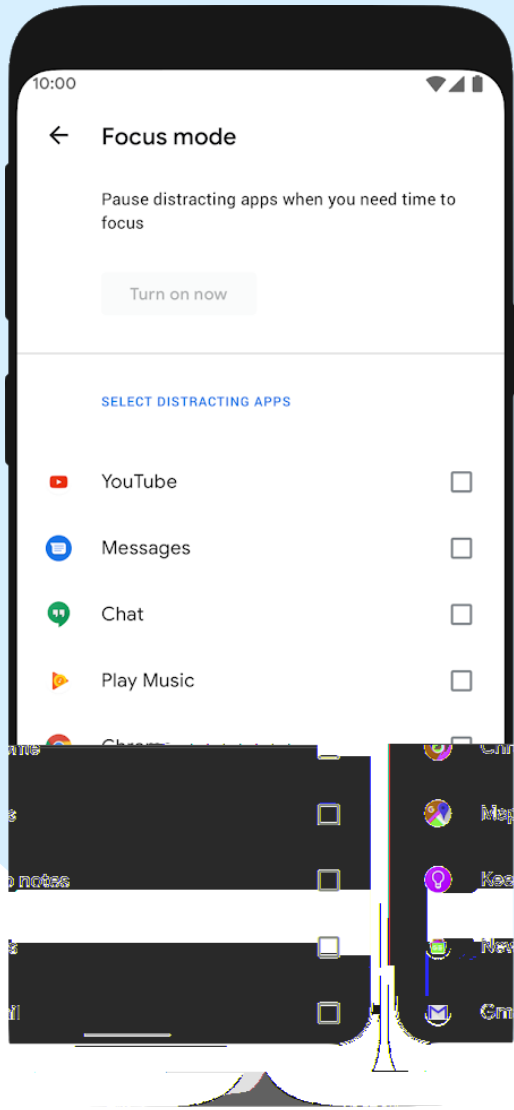
Trusted privacy

Employees have sometimes been hesitant to trust business-managed devices, especially when their private information and personal data is involved. That's why Android provides crystal clear separation of what's work and what's personal. With the Android work profile, IT only manages work apps and data, while the individual employee maintains full privacy and control of personal content and activity.*

Work-life balance

Digital well-being means balancing the ability to be productive from anywhere at any time with the need to unplug at the end of the day. Android's work-life divide means that work and personal apps are clearly labeled as such, and an employee can pause the work profile after business hours, on the weekend, or while on vacation. During the workday, tools like Focus mode help employees tune out distractions. There's even a well-being dashboard so employees can understand their usage habits and act on the data.
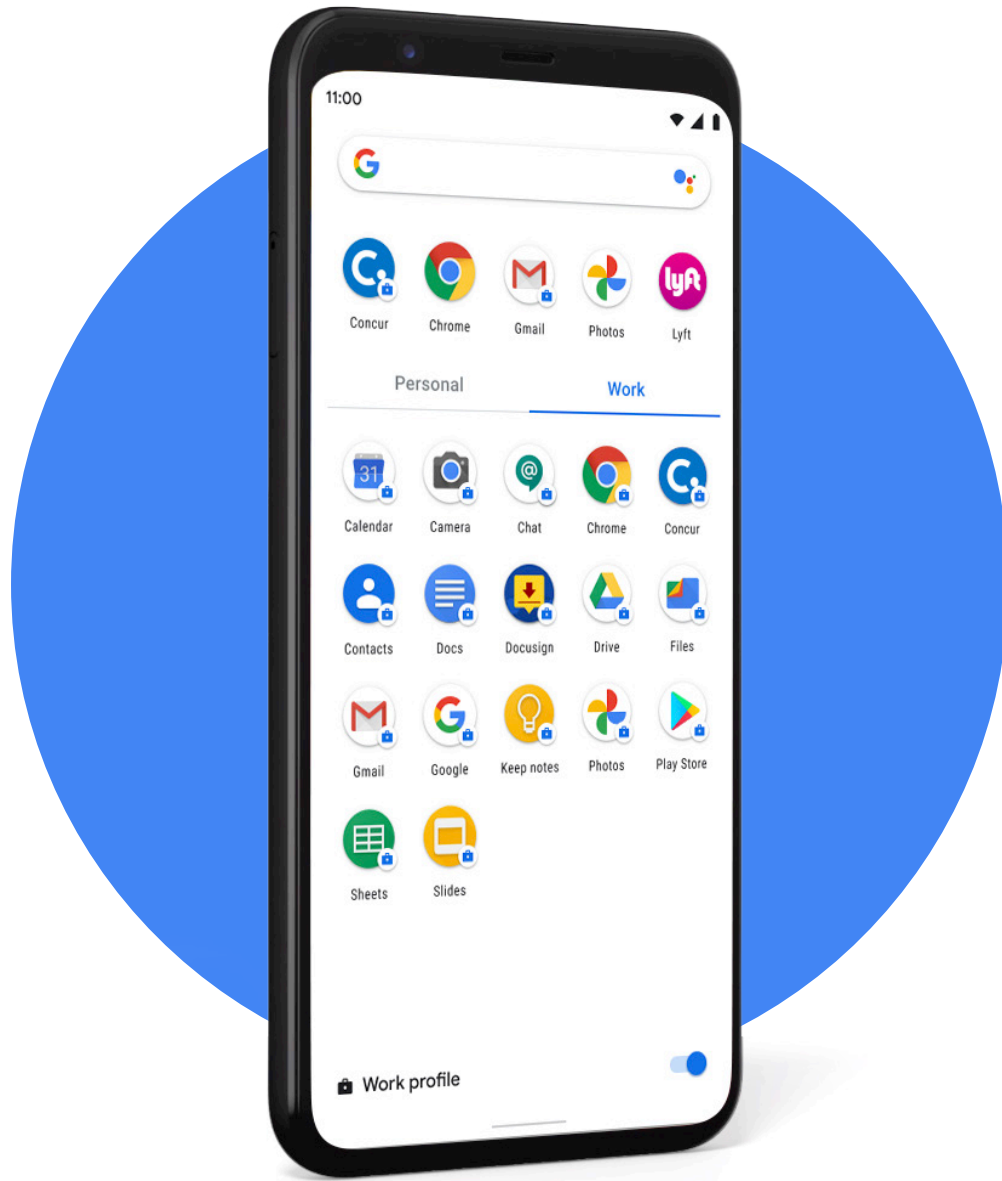
Easy onboarding

Having to learn a new set of tools or apps is not ideal for IT or for employees. That's why Android Enterprise leverages the Google tools users already know and love — like Gmail, Google Play, and Assistant — to shorten the path from onboarding to productivity. Apps like Gmail can exist in both work and personal profiles, making for a user experience that's familiar and seamless, while maintaining needed separation.

Helpful tools

With managed Google Play, IT teams curate a native app store stocked only with company-vetted and private apps to meet employee needs. And Android Enterprise devices are already loaded with helpful tools like Focus Mode, Google Assistant, Smart Reply, and Live Caption,[9] which provides real-time captions for video conference calls. All of these tools serve to help employees work smarter, not harder.

Use work profiles to support a healthier work-life balance

The Android work profile delivers OS-level security and separation that isolates work apps and data from personal apps and data. This separation gives employees a dedicated work environment that enhances privacy, productivity, and digital well-being. Work profiles provide employees with:

- Full privacy from IT on employee-owned and company-owned devices*
- Flexibility to pause work apps and take a break from work
- Ability to use managed Google Play as a dedicated enterprise app store

** On all personally-owned devices and Android 11 company-owned devices
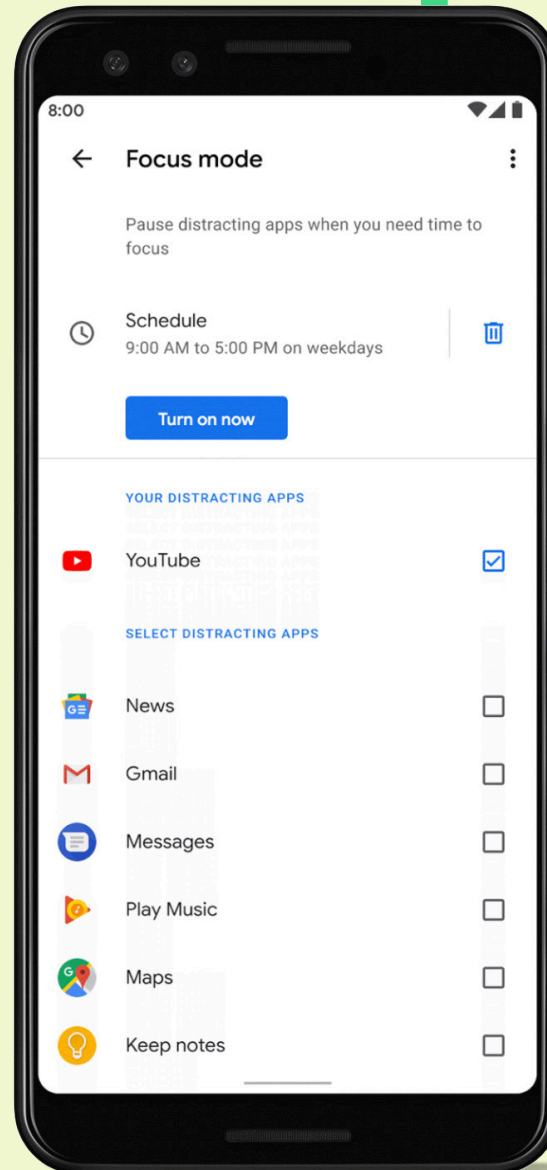
For organizations, work profiles allow IT to securely manage work apps and data, providing a consistent experience for employees on any device. The work profiles arms IT with:

- Strong data loss controls and anti-exploitation tools to isolate and protect enterprise data
- One easy-to-understand privacy model to build trust with employees
- A consistent management experience that reduces support costs
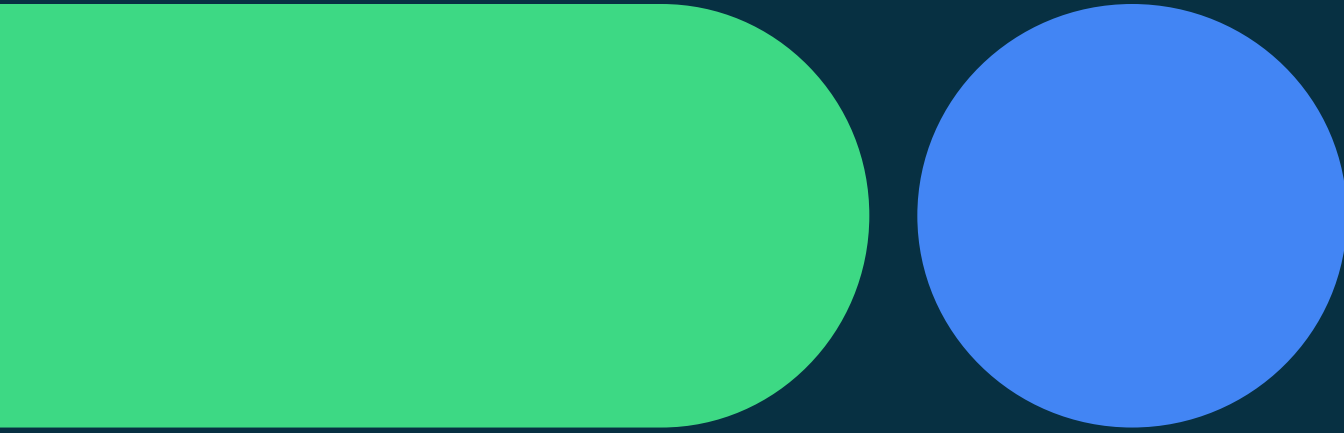
An open platform for device diversity and innovation at any price point

Android means choice and innovation

Digital transformation means more than just finding the right smartphone for your employees. It's also about unlocking untapped potential and opening new pathways to success. Other mobile platforms are closed systems, which limit device diversity and innovation.

Android's open and inclusive architecture means you can choose from a vast array of compatible devices to fit any use case and any price point. It also means harnessing the collective intelligence of Google-backed tools, resources, and expertise.
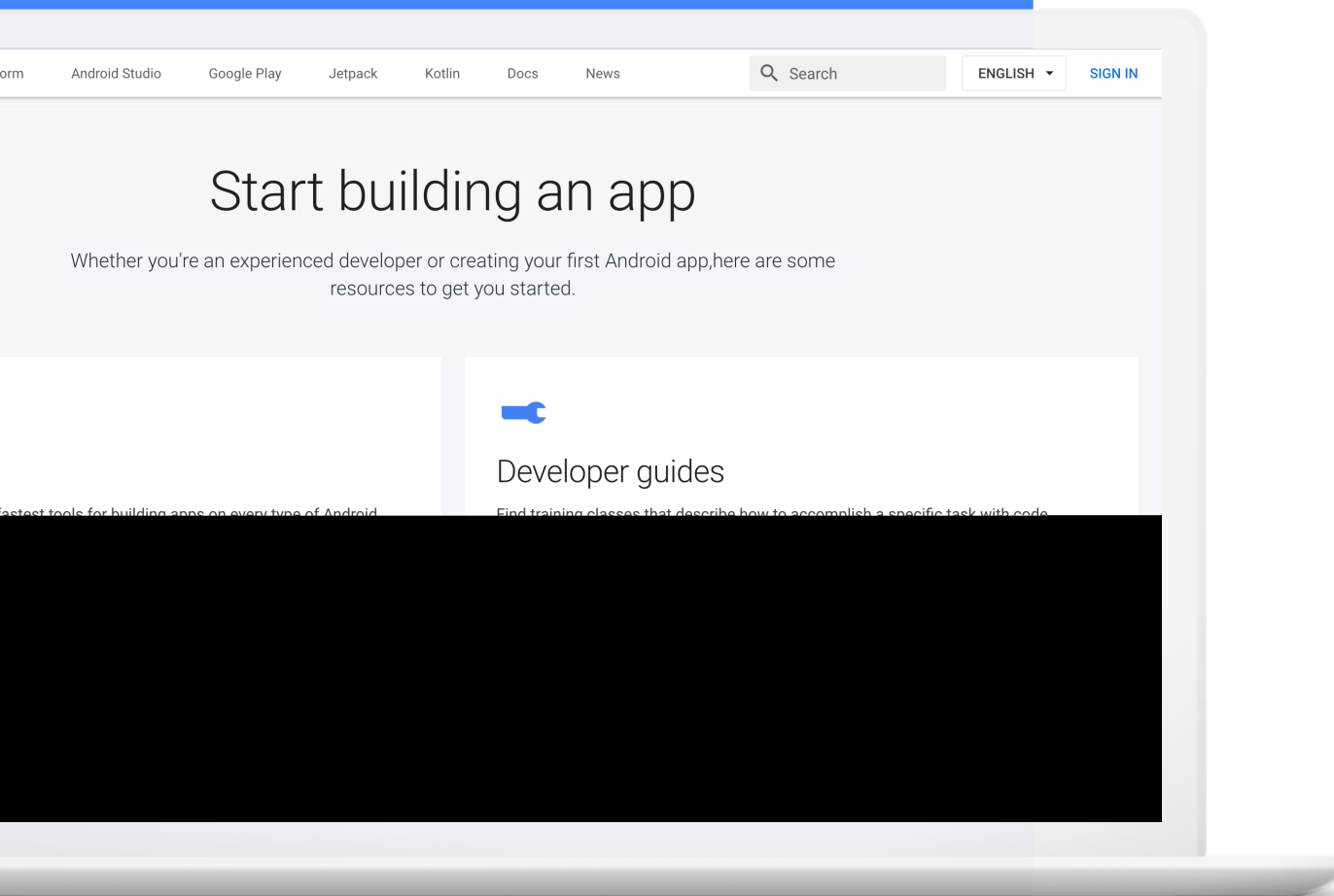
Developer tool to move faster and accomplish more

According to IDC, "Android's open nature allows for deeper integrations with third parties, which makes the platform more secure, dynamic, and, ultimately, of greater value to an enterprise."

Google's App Security Improvement program has helped developers strengthen the security of more than 1 million apps on Google Play. Also, Google works with 200 independent security researchers, white-hat hackers, and analysts to probe the Android code base for weaknesses and work together on implementing security updates.[10]

Development at speed

Leveraging Android's flexibility, openness, and common APIs, your in-house developers can build and deploy apps and solutions easily and quickly. IDC research showed that Android cuts the average time of development by nearly 50%[11] compared to iOS. And if your team needs collaborators, the world's largest developer community is standing by to help.

Scalability for any budget

The apps and solutions your team creates can be deployed seamlessly across your entire fleet, from knowledge worker devices to rugged field equipment. Android's scalability combined with its flexibility means that no matter your budget or device needs, you'll never be locked into short-term solutions that don't evolve with your business.

Google innovation

Unlock new possibilities for your business by harnessing Google's artificial intelligence and machine learning expertise. And with Google Cloud's intelligence portfolio, you could even discover new use cases with the potential to transform your business through augmented reality, virtual reality, Google Assistant, and voice-based tools like Dialogflow.

Advantages of Android's open system:

More stability and security for enterprise computing

55%[10] of Android mobile deployments "exceed expectations"

2x faster[11] average dev and deployment time for new enterprise apps (from **4.3 months** to **2.4 months**)

Scale & diversity

Android's scale means choice for businesses

Android delivers the flexibility businesses need to fully mobilize their workforce and handle every important need.

- **Device diversity:** Choose from hundreds of devices, at a range of price points, suitable for a range of tasks from knowledge work to point of sale

- **Open platform:** Android can leverage the expertise of OEM partners to develop highly specialized devices and tools to meet your exact needs. From field services, hospitality, and retail to manufacturing and healthcare

- **Common Android Enterprise APIs** mean there's consistent framework of security and manageability so you'll have a uniform experience across all your entire fleet

android

The New Android Enterprise

Expect more. Get more. Do more.

A look at the key benefits of Android:

Google-backed security and compliance you can trust to protect corporate data and meet future security challenges

Simple, consistent, and cost-effective to deploy and manage, even as you scale up and expand your needs

Empower employee productivity and digital well-being without sacrificing privacy or control

Provides the flexibility you need for ongoing innovation and digital transformation, allowing you to keep pace with competitors and to exceed the expectations of your customers

android

Android is ready to help you realize the full potential of enterprise mobility. With Android Enterprise, you'll not only get advanced solutions for today, you'll have a partner in creating innovative solutions for tomorrow's challenges.
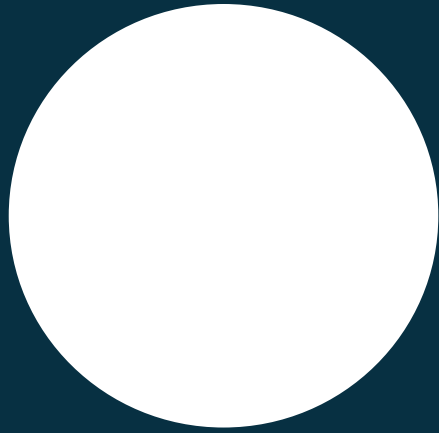
android 🤖

Take a look at all the possibilities for your business at android.com/enterprise

Have questions? Speak to a partner today and see how Android Enterprise can help your business meet the moment and move forward.

android

Sources referenced

1. ESG 2019 Digital Work Survey

2. Bitglass 2019

3. Mobile Security Index 2020, Verizon

4. IDC Worldwide Business Use Smartphone Forecast, 2017–2021

5. Mobile Security Index 2019, Verizon

6. Mobile OSs and Device Security: A Comparison of Platforms 2019

7. Google 2020

8. Owl Labs, State of Remote Work 2019

9. Features listed are standard on devices running Android 10

10. IDC 2019 Android For Enterprise Digital Transformation Opportunity

11. IDC 2018 Android: Poised to Take Mobile App Development to Next Level