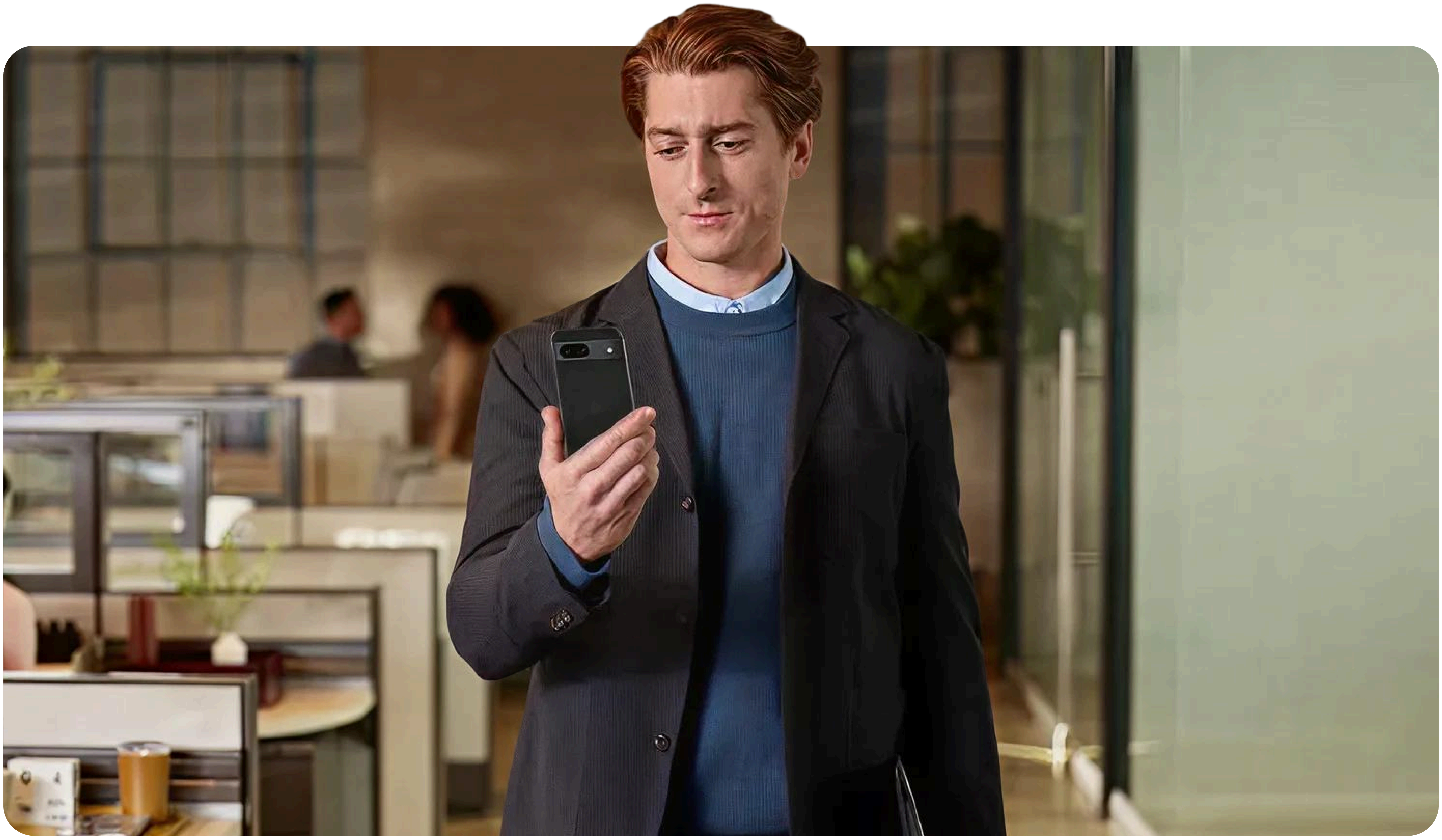
2026

Android Security Explained



Android

Table of contents

Executive Summary

For years, a common misconception in IT has been that Android is not secure enough for sensitive government and enterprise environments. This paper will demonstrate that this view is outdated and incorrect. Modern Android, combined with the **Android Enterprise** management framework, provides a multi-layered, transparent, and robustly managed security platform that is designed to meet the stringent requirements of government agencies and highly regulated industries.

> By the end of this paper, you will understand that Android is not only a viable option but a powerful and secure choice for deploying and managing mobile devices in any organization.

This document breaks down Android's security into five key areas:

01 **The Foundation of Trust**

How security is built directly into the device's hardware and the core operating system.

02 **Google's Protective Shield**

The always-on security services that protect devices from threats in real-time.

03 **Complete Enterprise Control**

How Android Enterprise gives you, the IT administrator, the granular control needed to enforce policy and protect data and explores how Android can integrate to your security architecture.

04 **Considering Android vs. iOS Security**

How Android's security model compares to Apple's, according to independent industry analysis.

05 **Government-Grade Validation**

The official certifications that prove Android's security meets high government standards.

The Foundation of Trust: Hardware and OS Security

Security isn't an app you install; it must be part of the device's foundation. Android requires hardware manufacturers to build security directly into the hardware and the operating system (OS), creating layers of defense that protect the device from the moment it's turned on.

Hardware-Backed Security

Think of software-based security as a safe sitting in an office: It's secure, but removable. Hardware-backed security can be thought of as building a bank vault directly into the foundation of the office building. It's immovable and secure, even if the room is broken into.

Verified Boot

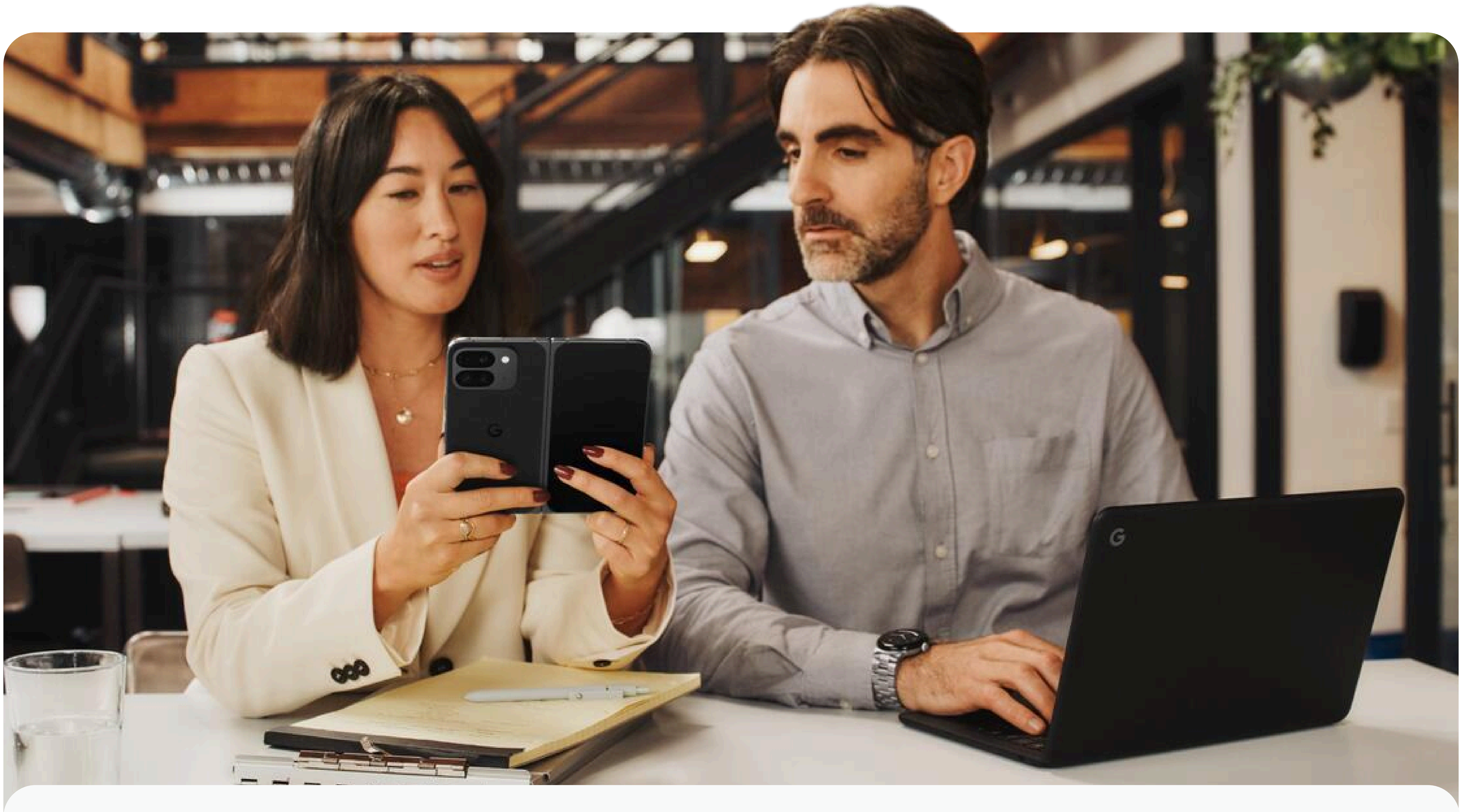
Every time an Android device starts up, Verified Boot runs a complete security check on the entire boot process. It ensures that the operating system hasn't been tampered with or corrupted by malware or exploited vulnerabilities. If it detects any unauthorized changes, it will warn the user and can prevent the device from booting, stopping an attack before it can even start.

Trusted Execution Environment (TEE)

Inside the phone's main processor is a special, isolated area called the TEE. You can think of it as a **digital vault** that runs separately from the main Android OS and has its own OS, processor, memory and storage. This is where the most sensitive data, like encryption keys and biometric information (fingerprints, face scans), is processed and stored. Even if the main OS were somehow compromised, it cannot access the contents of this secure vault.

A hardware-backed KeyStore

A fundamental and crucial requirement for achieving a high level of security in the Android ecosystem. While the Android Keystore system itself provides APIs for secure key management, the hardware-backed implementation is what truly isolates cryptographic keys from the main operating system (OS) and offers robust protection against advanced attacks.



A Hardened Operating System

The Android OS itself has powerful, always-on security features that protect your data and apps.

Application Sandboxing

Imagine every app on your phone lives in its own **fenced-in yard.** It can do whatever it wants inside its own yard, but it can't see or touch what's happening in the neighbors' yards. This is called sandboxing. An app cannot access the data, files, or memory of another app unless the user grants explicit permission. This crucial feature contains the damage a malicious app can do, preventing it from stealing data from your email, banking, or other critical applications.

Security-Enhanced Linux (SELinux)

Running deep within Android is a security system called SELinux. Think of it as a **security guard with a very specific list of rules** for every single process running on the device. It enforces strict "access control" policies, meaning processes are only given the absolute minimum permission they need to do their job. This makes it incredibly difficult for attackers to gain control of a device even if they find a vulnerability in a single app or service.

Android's memory safety

is all about preventing the most dangerous types of bugs—where apps accidentally corrupt or misuse the phone's memory. Think of it as **building the Android house with safer materials** (using programming languages like Rust) so the walls (code) won't crumble. Additionally, it uses **security guards** (like Control Flow Integrity and Memory Tagging Extensions) to constantly monitor and immediately stop any app trying to peek at or change memory that doesn't belong to it. This greatly reduces the biggest source of security flaws.

Google's Protective Shield: Services and Intelligence

On top of the strong foundation, Google provides a layer of intelligent security services that actively defend devices against evolving threats.

Google Play Protect

This is Android's built-in, always-on malware protection. You can think of it as an **antivirus and security scanner for the device**, powered by Google's massive scale in machine learning which allows it to scan over 200 billion applications every day.

- **Before Installation:** It scans billions of apps in the Google Play Store to ensure they are safe before you ever download them.
- **On Your Device:** It continuously scans the apps already installed on your device, looking for any signs of malicious behavior.
- **Automatic Action:** If Google Play Protect finds a Potentially Harmful Application (PHA), it can automatically disable it or remove it from the device to keep your data safe.

> This service works silently in the background, protecting every certified Android device with Google Mobile Services, whether it's a personal phone or a corporate-owned asset.

Timely and Consistent Security Updates

In security, speed is critical. A known vulnerability must be patched quickly before it can be widely exploited. Android has a robust system for delivering security updates.

Regular Security Patches

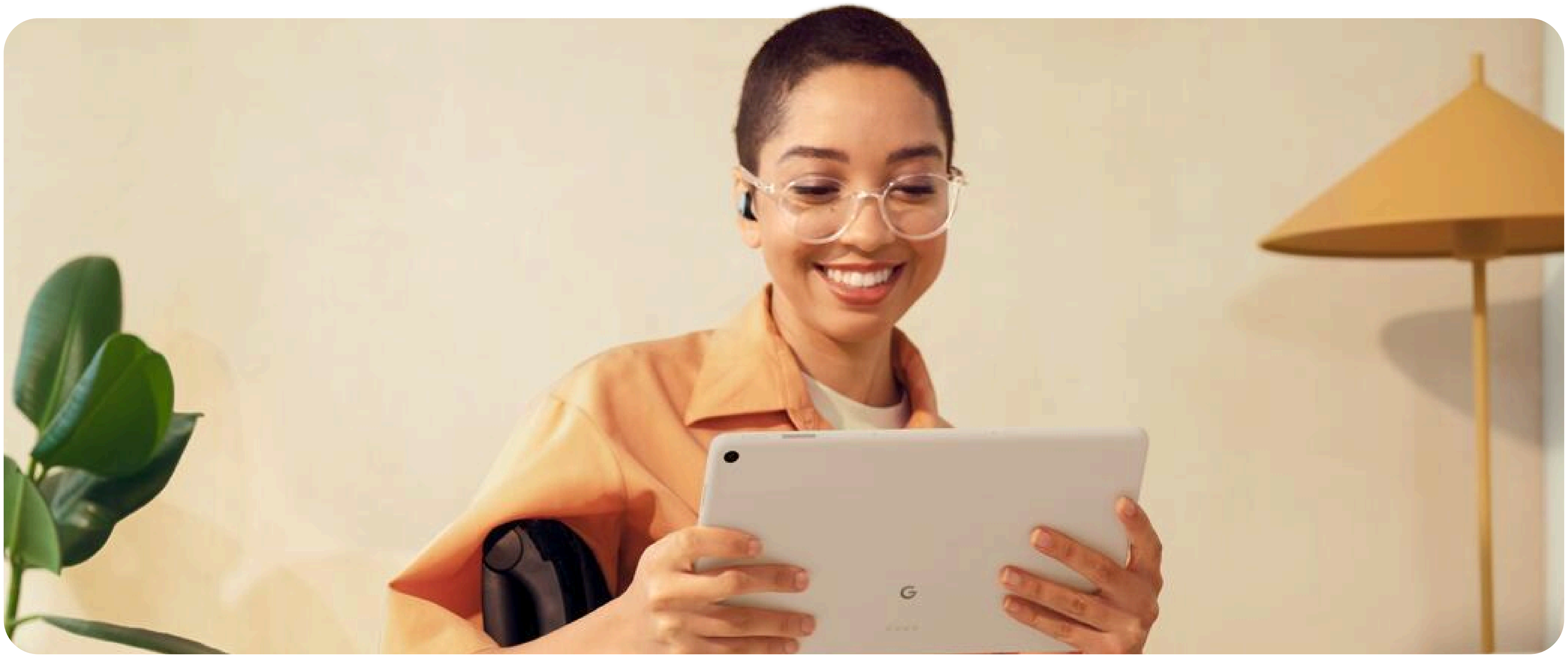
Google and its hardware partners release security updates for Android that fix newly discovered vulnerabilities.

Project Mainline (Google Play System Updates)

In the past, all security updates had to come from the device manufacturer and carriers, which could sometimes cause delays. Project Mainline solves this. Think of it like a normal app update: Google can deliver updates for critical OS components, such as Bluetooth, networking, or multimedia libraries, **directly through the Google Play Store,** without needing a full OS update from the manufacturer. This means crucial security fixes get to your devices faster, more reliably and in a nonintrusive manner than ever before, dramatically reducing the window of opportunity for attackers.

Google Play App Updates

Unlike other platforms, Google is able to patch common vectors of attack, such as Google Chrome or Webview, without having to update the operating system. This allows an organization to protect the device from attack by limiting the attack surface, even if the underlying OS vulnerability has not yet been patched.



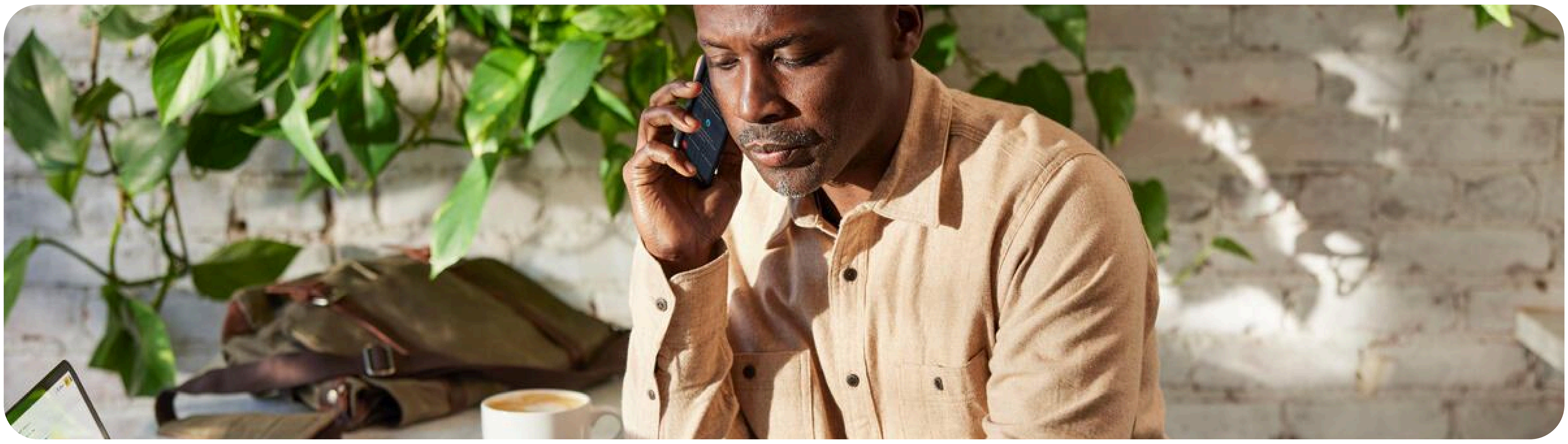
Complete Enterprise Control: Android Enterprise

A secure platform is only useful if IT can manage it. **Android Enterprise** is the framework that provides administrators with the tools they need to secure, deploy, and manage Android devices at scale. This is all done through your organization's central management console, known as an EMM (Enterprise Mobility Management) or UEM (Unified Endpoint Management) solution.

The Power of the Work Profile

The work profile is the cornerstone of Android's approach to securing corporate data, especially for Bring Your Own Device (BYOD) scenarios or when users can use personal applications own company-owned devices (COPE).

> **What it is:** The work profile creates a **separate, encrypted container** on a user's device that isolates work apps and data from their personal apps and data.
>
> **The Analogy:** Think of it as a **secure briefcase inside a personal car**. The company has full control over the briefcase—it can add or remove items, lock it, and even destroy its contents remotely if it's lost. However, the company has no visibility or control over anything else in the car. The user's personal photos, messages, and apps remain completely private and untouched.
>
> **Key Benefits:** This separation means you can secure company data without infringing on employee privacy. You can wipe all corporate data from a device without touching a single family photo.



Comprehensive Device Policies

Through your EMM/UEM console, Android Enterprise allows you to enforce hundreds of security policies on both work profiles and fully managed company-owned devices. You are in complete control.

Common policies you can enforce include:

- **Password Enforcement:** Require strong passwords or passcodes with complexity rules and set an expiration cadence.
- **Mandatory Encryption:** Ensure all data stored on the device and within the work profile is encrypted.
- **Network Security:** Configure secure Wi-Fi networks and force all work-related traffic through a company VPN.
- **Data Loss Prevention (DLP):** Block users from copying/pasting data between work and personal apps, or prevent screenshots of sensitive information.
- **Application Management:** Silently install, remove, and update work apps without any user interaction. You can also block the installation of unauthorized apps.
- **Remote Actions:** Remotely lock a device or wipe all corporate data if a device is lost or stolen.

Connecting Android to your security infrastructure

While mobile administrators may work routinely in the EMM/UEM console, enterprise security and operations (SecOps) teams often use different tools. These tools provide a bird's-eye view of security across a company's infrastructure, not just mobile. Fortunately, **Device Trust from Android Enterprise** allows you to easily connect both managed and unmanaged (those not enrolled to a EMM/UEM platform) devices to your security infrastructure.

Using Device Trust from Android Enterprise, security partners can inspect the state of the device, understanding common issues like whether the device is current with security updates, or whether the user has a proper device lock code set.

Here's how:

- **Identity systems:** Partners that leverage Device Trust can determine, when a user logs into an enterprise application through an identity provider (IDP), whether the device is secure. The IDP can also periodically re-check the security state of the device and log the user out of enterprise apps if necessary.
- **Threat detection systems:** Endpoint Detection and Response (EDR) as well as Mobile Threat Defense (MTD) partners that leverage Device Trust can bring Android security signals so SecOps teams have a holistic view of security, including mobile. Device Trust also provides unique identifiers to improve correlation of devices with other security systems for improved forensics and correlation capabilities.
- **Security monitoring systems:** Security monitoring tools, such as security information and event management (SIEM) tools, can use Device Trust to better correlate devices as well as obtain better context for security events. For managed devices, improved access to device logs, such as security and network logs, from the device is also provided.

Considering Android vs. iOS Security

While a layered security model is excellent in theory, its real-world effectiveness must be validated by objective, third-party experts. Recent in-depth reports from independent security analysts have directly compared flagship Android and Apple devices, and the results challenge long-held assumptions. These analyses bolster the case for Android as a leading platform for enterprise and government security.

Leviathan Security Group: Mobile Platform Fraud Prevention Assessment (Oct 2025)

Leviathan Security Group, a respected security consultancy, conducted a study to perform a deep-dive assessment of the fraud and phishing protections built into both Android and iOS. The full study was commissioned and funded by Google. This type of security is critical for government and enterprise, as social engineering remains a primary vector for attacks.

> **Key Finding:** The most recent assessment, which tested devices like the Google Pixel 10 Pro, Samsung Z Fold 7, and Apple iPhone 17 Pro (on iOS 26), found that **Android smartphones scored highest** for built-in scam and fraud protection features. All tested Android devices excelled with on-device AI detection of suspicious message patterns and advanced screen-sharing protection that prevents sharing sensitive information like OTPs.
>
> **Why it Matters:** While both Android and iOS provide essential security controls, Leviathan's specialized analysis shows that **Android maintains a distinct advantage in providing proactive defense** against social engineering and fraud. Features exclusive to Android devices, such as AI-powered in-call scam detection and enhanced Safe Browsing with LLM-powered warnings, proactively protect users from making critical errors, making it a top-tier choice for organizations prioritizing proactive threat prevention.

Counterpoint Research: Assessing the state of AI-powered mobile security (2025)

Counterpoint Research, a global industry analysis firm that specializes in delivering in-depth intelligence on the technology, media, and telecom (TMT) markets, analyzed how Artificial Intelligence (AI) is transforming mobile security from reactive to proactive measures. With attackers increasingly using AI to thwart defense efforts, it's critical for platform providers to use AI to protect against emerging threats.

> **Key Finding:** According to a recent evaluation of native smartphone security features, Android smartphones offer a greater number of **AI-powered protections, particularly compared to iOS**. These features cover multiple key areas, including real-time, on-device detection of scams in calls, messages, and web browsing (via Play Protect and Gemini Nano). This investment by Google on proactive measures powered by AI, according to the report, "helps Android stay on even footing with potential attacks – if not ahead of them."
>
> **Why it Matters:** This focus on proactive, AI-driven security directly addresses top consumer concerns, as a Counterpoint study indicated that 77% of users have a "More Positive" perception of integrating AI for "Scam detection & protection" than any other feature listed, highlighting the critical value users place on this capability. The continuous effort to utilize increasingly powerful AI tools positions Android OEMs well to combat rising sophisticated threats and connects with user concerns.

Omdia Mobile Device Security Scorecard 2024

Omdia, a leading technology research firm, conducts an annual hands-on evaluation of the security features of major smartphones. Their 2024 scorecard directly compared the top devices in the market.

Read the Mobile Device Security Scorecard 2024

> **Key Finding:** In this assessment, **Google's Pixel 9 Pro and Samsung's Galaxy S24 scored higher for their security features than Apple's iPhone 16 Pro.** The testing methodology combined hands-on analysis by penetration testing professionals with data on which security features are most important to users.
>
> **Why is Matters:** This result demonstrates that, based on a rigorous and objective evaluation, Android's implementation of security is not just comparable to, but in some cases superior to, its primary competitor.

Conclusion: A Secure, Flexible, and Validated Choice

Android provides a modern, layered approach to security that is more than capable of meeting the needs of government and security-conscious enterprises.

Key Takeaways

- **Security is Built-In, Not Bolted On:** From hardware-level Verified Boot to the sandboxing and access controls of the OS, Android is secure from its very core.
- **Multiple Layers Work Together:** Hardware security, OS hardening, memory safety, Google's intelligent services, and your enterprise management tools combine to create a defense-in-depth security posture.
- **Control Without Compromise:** Android Enterprise, particularly through the work profile, gives you the powerful controls needed to protect sensitive data while still respecting employee privacy on personal devices. Over 150 EMM and UEM partners support Android Enterprise today.

- **Officially Validated and Certified:** Don't just take our word for it. Android's security has been rigorously tested and validated by independent labs and government bodies. Key certifications include:
  - **FIPS 140-2:** This certification validates the strength of Android's cryptographic modules, which are used for encryption. This is a common requirement for U.S. federal agencies.
  - **Common Criteria (ISO/IEC 15408):** Many Android devices have achieved Common Criteria certification, which is an international standard for IT security.
  - **DoDIN Approved Products List (APL):** Many Android devices are on the U.S. Defense Information Systems Agency's list of approved products for use on DoD networks. As of October, 2025, Apple was not listed in this program.
  - **Commercial Solutions for Classified (CSfC):** Many Android devices are on the U.S. National Security Agency's list of approved products.
- **A strong ecosystem of partners:** Through the Android Enterprise framework, devices that run Android can be connected to leading EDR, IDP and other security systems. This allows organizations to obtain enhanced visibility over Android devices across an enterprise's security infrastructure, whether the devices are managed or unmanaged.