Mobile, App, and IoT security

Protecting data and devices worldwide

With the dramatic rise of state-sponsored cyber attacks and malicious actors online, we believe our products and services are only as helpful as they are secure. At Google, we are more focused than ever on protecting people, organisations and governments by sharing our expertise, empowering society to address ever-evolving cyber risks and continuously working to advance the state of the art in cybersecurity to build a safer world for everyone.

As such, it's imperative for us to stay ahead of the curve and constantly evolve our security solutions to tackle the ever-growing threat landscape, particularly when it comes to securing all connected devices and apps, in order to provide consumers with a safe environment where they have agency and choice in the devices they engage with.

Challenge

Connectivity comes with a price

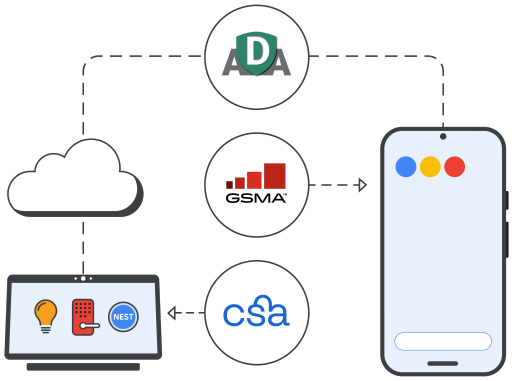
We conduct so much of our daily lives from our smartphones, apps, and IoT devices—spending more and more time online and sharing more and more valuable data, such as banking or healthcare information, in the process. Because of this, sophisticated cybercriminals are targeting these devices more than ever before to obtain sensitive information.

More devices, more data—more threats

There are now an estimated 17 billion IoT devices devices in the world, from printers to garage door openers, each one packed with software (some of it open-source) that can be easily hacked.[1] Overall, the number of compromised IoT devices almost doubled in 2020.[2]

- Although we are becoming deeply connected through IoT devices, there are no global standards for measuring the security quality of connected products, leaving consumers to make uninformed device security decisions.
- Consumers should have the right to transparency about their digital products just like they have the right to know what ingredients are there in the food or cleaning supplies they purchase.
- Mobile devices are just one vector to other attack surfaces, and the interconnectivity of devices increases the need for security transparency at scale. Hence, the security of the connected device ecosystem is as important as the security of networks and systems.

Our collaboration with industry organisations



Our solution

At Google, we're advancing the security and transparency of our connected devices through mobile, app, and IoT security:

Mobile security

Android, our open source operating system, leverages a layered security approach to keep mobile devices safe:

- Layered security
  - Verified Boot, roll-back protection, and factory reset protection ensure the latest, safest Android version.
  - PIN and biometric authentication shield against outside access.
  - 'Find My Device' helps locate the device or wipe it clean if it's
  - stolen or lost.
- Identity and password protection
  - 2-step verification, using your phone as a security key and Password Manager shield your Google account against outside access.
  - Security checkup and optional advanced protection keep the device running safely and smoothly.
- Anti-phishing protection
  - Phone by Google and Messages by Google help detect and prevent scam and phishing attacks.
  - Google Safe Browsing safeguards over 5 billion devices globally.

App security

Out-of-the-box anti-malware helps keep bad apps out and data safety information provides transparency to users when downloading apps.

- Google Play Store: Machine-learning detection tools and human analysts review all apps before they're available for download. The data safety section explains what types of data apps collect and what that data is used for.
- Google Play Protect: Scans more than 125 billion apps every day and notifies, removes, or disables if security risks are detected.
- App Defense Alliance (ADA): Google worked with top mobile threat detection partners to launch the App Defence Alliance that helps safeguard Android users from Potentially Harmful Applications (PHAs) through shared intelligence and coordinated detection.

IoT security

IoT security labels clearly convey privacy and security practices on a device, like what data is being collected.

- We believe in five core principles for IoT security labeling schemes: live label, evaluation schemes, security baselines coupled with flexibility, broad-based transparency and adoption incentives.
- We are working with the Connectivity Standards Alliance (CSA) and GSM Alliance (GSMA) to standardise an industry-wide certification programme for existing and future regulatory requirements.

Our principles

At Google, we apply three core principles to advance the security and transparency of our connected devices:

Defense in depth: We utilise multiple layers of security architecture that work together to build a strong defense that runs smoothly and effectively.

Open & transparent: Transparency is key to our philosophy. By keeping our platform users informed and sharing knowledge to bolster our protection, we believe an open source ecosystem can be more secure than a closed one.

The best of Google and our ecosystem: We partner with expert teams across Google and the industry to help keep billions of users safe.

Applications

IoT security labels: putting control in consumers' hands

Without established IoT security labelling, there are no global standards for device manufacturers to follow. Users also don't have the visibility they deserve into whether their devices protect their data. The industry needs to come together to push IoT security forward and put control back in the consumers' hands. We're working towards an IoT security labelling scheme through our processes and partnerships.

First, we invest in outside security research to pinpoint possible vulnerabilities (Google Nest participates in the Google Vulnerability Reward Programme and provides rewards for security researchers outside Google who find vulnerabilities).

From there, we issue critical bug patches and fixes for at least five years after launch.

All our devices developed in 2019 and beyond use Verified Boot to ensure the right software is running and access is protected. For example, our Google Nest devices are validated using third-party, industry-recognised security standards, like those developed by NIST, ETSI, and ISO.

These standards, and our secure software development life cycle (SDLC), reduce the likelihood that consumers will be exposed to poor security practices and pave the way for an open, safer Internet.

Our industry investments and milestones

2007 Safe Browsing established to proactively alert users when they visit dangerous websites and now protects over 5 billion devices.

2010 Google Transparency Report launched to show how governments and corporate policies and actions affect privacy, security, and access to information online. In 2018 we added an Android-specific transparency report.

2017 Launched Google Play Protect which is now the most widely deployed anti-malware solution scanning over 125 billion apps a day across 3+ billion devices.

2019 Security Key introduced as a built-in feature on Android and then for iPhone in 2020.

2022 Google Play launched a data safety section to give people more information about how apps collect, share and secure users' data and initiated the first badge system for any app that has completed an independent security review through the App Defense Alliance.

2023 Passkey: the passwordless future is being set into motion with extended passkey support after a decade of driving open standards with the FIDO Alliance and tech leaders worldwide.

Our approach

Committed to an open, secure digital world

Security concerns will only heighten with more data on more devices across different networks. We're helping advance the future of connected device security through our product development, transparency criteria, and industry partnerships.

A cornerstone of our product strategy is ensuring our products are secure by default. Safe Browsing, Google Play Protect, and built-in security keys protect mobile devices and apps to give the highest level of security in our products.

We help democratise security operations by being open and transparent in how we tackle issues and sharing connected device security knowledge. We believe an open source ecosystem can be more secure than a closed ecosystem with our layered security approach.

By collaborating within CSA, ADA and GSMA, we strive to advance the state of the art in cyber security for a safer Internet and future for all.

We are committed to raising the bar for connected device security and setting the standard for a safer online environment for everyone, everywhere. Learn more about Google's progress in connected device security: g.co/connecteddevicesafety

Sources: [1] CNBC Cyber Report, 9 January 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, 20 July 2021