Publication date:
October 2023
Authors:
Aaron West
Hollie Hennessy

Mobile Device Security 2023

Annual buyer's scorecard assessing the security of the leading mobile devices

Contents

Summary

Google's Pixel 8 beats other leading phones in security feature testing

Google's Pixel 8 smartphone scored ahead of Apple's iPhone 15 and other leading Android-based devices, including the Samsung Galaxy S23, OnePlus 11 5G, Xiaomi 13 and Huawei P60, in Omdia's annual Mobile Device Security Scorecard (see **Table 1**), which compares key security features from leading smartphones, including anti-malware protection, network security, and secure backups.

The total ratings are based on hands-on testing by Pen Test Partners combined with consumer importance weightings from a survey of 1,578 consumers across 13 major countries in the Americas, Asia & Oceania, and Europe.

Table 1: Smartphones rated for their security features

Feature	Consumer importance weighting	Ideal score	Google Pixel 8	Samsung Galaxy S23	OnePlus 11 5G	Xiaomi 13	iPhone 15	Huawei P60
Anti-malware protection	15%	100	100	100	100	100	100	100
Files and photo protection	14%	100	100	100	100	100	50	100
Network security	13%	100	100	75	50	50	50	25
Identity protection	12%	100	100	75	50	50	75	50
Anti-phishing protection	10%	100	75	75	75	75	50	0
Hardware security	9%	100	100	75	75	75	75	75
Lost device protection	8%	100	100	100	75	75	100	75
Security updates	6%	100	100	100	75	75	75	25
Security awareness and remediation	5%	100	100	100	100	100	25	100
Secure backups	4%	100	100	75	100	50	75	25
Physical access control	3%	100	100	100	75	50	100	100
Parental control	1%	100	100	100	100	100	100	75
Weighted total	**100%**	**100**	**97**	**88**	**79**	**76**	**70**	**62**

Source: Omdia

Key findings

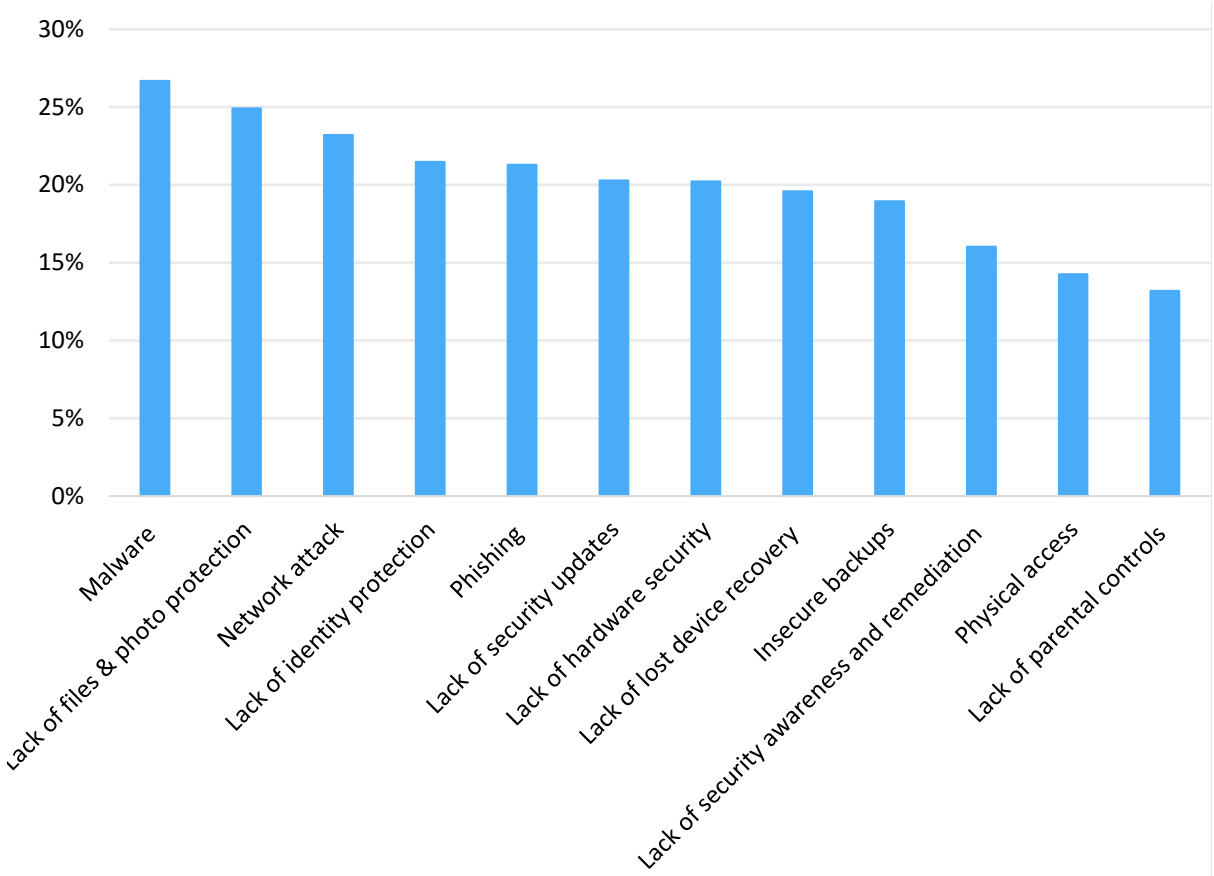
The Google Pixel 8 did well in all the security features we tested, only losing marks for anti-phishing protection. It could not detect customized phishing emails or SMS messages—a test that no other tested phone passed either. Regarding malware protection, Google users can easily enable download of unauthorized applications, although there is a warning that needs to be bypassed. If the file is known to be malicious, Google correctly identifies it and flags a warning. While still scoring full marks for physical access control, the Google Pixel 8 uses an optical fingerprint sensor rather than a more-sophisticated ultrasonic one. However, testing these sensors against each other for efficacy was beyond the scope of this test.

Samsung's Galaxy S23 scored second highest in our testing, with full marks in a number of security features, including lost device protection and files and photo protection. Identity protection was an area in which Samsung did not perform as well because it does not offer two-factor authentication (2FA) through a call or FIDO U2F (fast identity online universal 2nd factor); also, its proprietary password manager does not proactively check saved passwords for compromise.

Apple's iPhone performs differently to all the other phones tested because it is not based on Android and has its own App Store. While the iPhone 15 did well in security testing and most areas, it lost significant marks for not detecting more-basic, automated phishing emails, texts, or calls; not offering a clear audit trail of account activity; and not having centralized security notifications, or automatically revoking permissions for unused apps (within "security awareness and remediation").

Many Android features and capabilities are repeated across Android devices. It is worth noting that although Huawei has its own operating system, HarmonyOS, it uses the Android system (based on Android Open Source Project) in most parts of the world, which was the system used in our testing. But where Huawei adds its own solutions instead of using Google's, these often lack the same levels of protection.

Figure 1: Security concerns and how commonly consumers rated them "very concerning"



Source: Omdia

Consumers rated malware as the most concerning security issue in our survey (see **Figure 1**), followed by lack of protection for files and photos (a new topic covered in this year's scorecard), and network attack. Similar to last year's survey, network attack ranked third whereas malware went from being one of the less important concerns to the most important.

Interestingly, although consumers were most concerned about malware, they also had high confidence that smartphones could address the issue—with 66% rating them "very effective," or "effective." This rings true with our testing—all the phones prevented malicious applications from being installed, either by correctly flagging the application as malicious or making it very difficult for the user to sideload applications in the first place.

Phishing rose towards the top in the 2023 survey, having previously been second to last. This could be explained by an increase in phishing attacks against consumers, including the rise of smishing and spear phishing attacks, which consumers may have become more aware of through media, friends, and family. Identity protection was the most important security feature to consumers when surveyed last year—and it is still of high concern, but now in fourth place.

Table 2: Security concerns covered in Omdia's consumer survey

Feature	Description
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to your smartphone and the data that resides on it.
Lack of files & photo protection	The lack of an additional layer of protection for various files or photos that may be stored on your device.
Network attack	An attack on the communications from your smartphone to various cloud services, and your connection to the internet overall. An attack could result in the transfer of data over the internet being intercepted or spied on.
Lack of identity protection	Poor protection involving passwords for apps and websites, or a lack of information when your password has been stolen or breached. Fewer layers of identity protection, which can result in breached credentials.
Phishing	A tactic, including fraudulent emails, texts, or phone calls, used by bad actors to trick individuals into revealing personal information such as passwords and credit card numbers.
Lack of security updates	A lack of updates to fix issues within your smartphone's software that could be used by bad actors to corrupt your device or steal information from it.
Lack of hardware security	A lack of smartphone hardware to offer higher levels of protection for sensitive data that resides on your device.
Lack of lost device recovery	A lack of features enabling you to locate, track, lock, or even remotely wipe a lost or stolen device.
Insecure backups	A lack of encryption of backup data while it is being transmitted off your device to various cloud services or when residing in a cloud service.
Lack of security awareness and remediation	A lack of information on your device warning you about potential security-related issues and providing steps to remedy those issues.
Physical access	Bad actors gaining unauthorized access to your device by either presenting an artificial copy of your fingerprint or by trying repeatedly to guess your passcode.
Lack of parental controls	A lack of features enabling you to configure or set various restrictions on your children's smartphones and the services/apps that run on them.

Source: Omdia © 2023 Omdia

Test results

Anti-malware protection

All phones prevented malicious apps from being installed, either through detection or by making it very difficult for the average user to sideload apps at all.

With Android devices, users are warned about enabling installation of third-party devices; however, this is easily bypassed, and the user can install the selected application afterwards. OPPO OnePlus and Google phones rely on Google Play Protect, which correctly identifies when malicious applications are being installed—but again this can be ignored by the user with a single press.

Huawei, Samsung, and Xiaomi implement their own anti-malware scanning solution for app installs, with Samsung and Xiaomi having two levels of protection, with both their own custom solution and Google Play Protect working in tandem.

Apple iOS acts differently to all the others; Apple's App Store prevents sideloading of applications unless you have an enterprise app developer certification. Because this is a consumer test, this was not covered. It should be noted that Apple has complete control over which apps consumers can install on their phones and that the App Store will automatically prevent any malicious apps from being listed and installed in the first place.

Files and photo protection

For file protection, such as PDFs, all devices except the iPhone allow miscellaneous files to be protected within their built-in applications. The iPhone does not allow files to be secured locally and hidden behind additional layers of authentication.

All tested devices allow users to protect chosen images on the device, such as putting them in a hidden gallery that requires biometrics to access.

Network security

Web traffic can be observed on all devices if a proxy is configured to view unencrypted traffic. For encrypted traffic, a certificate authority (CA) needs to be installed. On all Android devices this would require some form of modification via a rooted device, unless an application has specifically opted in to trust other certificates, such as those in the user-modifiable CA store. On the iPhone, users can accept warnings to be able to install their own development certificate and intercept traffic.

Only the Google Pixel 8 and Samsung Galaxy S23 allow the user to disable 2G in settings (Samsung through selecting "3G only." On the iPhone 2G can only be disabled by putting the phone in lockdown mode.

All devices except the Huawei P60 support eSIMs and all applicable eSIM options. This mitigates the ability of an attacker to remove the SIM and network connectivity from a stolen phone.

While all devices can support VPNs, the Google Pixel 8 is the only device with a built-in VPN that can be set to “always on.” On all other devices, you would first need to install a third-party (possibly paid-for) VPN.

Identity protection

All devices, on installation, include manufacturer-provided accounts, although they do vary in features and functionality.

For the Xiaomi 13 and the OPPO OnePlus 11 5G, the user is prompted to log in or create both a Google account and a manufacturer account. Both manufacturer accounts lack their own security features and capabilities, such as password managers, but users can simply opt for Google’s offering instead, which includes all the expected security features.

The Apple iPhone 15 and the Huawei P60 include account security and the use of 2FA but lack account check-up features and auditability. For example, on the iPhone you cannot see a clear audit trail of all account activity. However, in iCloud Keychain Apple provides a well-used and functional password manager, and support for passkeys for all accounts that support them.

Anti-phishing protection

More-sophisticated spam attacks with customized content are unavoidable and unlikely to be blocked by a mobile device’s automated system, which was confirmed in our testing when no device detected them. Commonly repeated spam attempts should be blocked, but multiple devices failed to do so.

When receiving a harmful link, devices should have a fallback beyond the receiving app (such as Messages) to protect the user. An example of this is the Google Chrome or Samsung Internet browser giving a second warning after the initial app did not detect that the link was malicious.

The Huawei P60’s built-in apps failed to protect the phone from any malicious links and messages. The browser did not even warn against known malicious URLs, which are on phishing site lists.

Apple’s built-in apps, such as iMessage and Mail, also offered little protection. However, the Safari browser did block known malicious URLs, so users would be warned even if the apps had failed to detect an attack.

Hardware security

All phones have a hardware security module. The iPhone uses Secure Enclave; the Google Pixel 8 has two modules—the Tensor security core and Titan M2; and all other phones use the Qualcomm Secure Processing Unit (SPU).

It is difficult to perform direct comparisons across different manufacturers’ security modules and their implementations. Even when using the same chip, such as the Qualcomm SPU, the interfacing

software is entirely different and supports different features. Although Google's Tensor security core and Titan M2 chips implement further layers of hardware security beyond other offerings, the Titan M2 is physically separate from the main system on a chip (SoC). Like other designs, Apple's Secure Enclave physically segregates secure processing from the main device processor.

Although Google has added an extra layer of hardware security protection to its Pixel 8 devices, thus gaining a higher score, a singular hardware security unit can also provide adequate protection for user data.

Lost device protection

All tested phones provided in-depth tracking, location, wiping controls, and the ability to leave a message on the display for lost devices.

The Huawei, Xiaomi, and OnePlus devices did not support offline tracking. All except the Huawei P60 support notifying users of unwanted trackers, such as AirTags, nearby. The iPhone, Google Pixel, and Samsung Galaxy S23, which support tracker warnings, also allow a sound to be played through the tracker and explain to the user how to disable it once found.

The OnePlus 11 5G relied on Google's application only; however, it still supported most features.

Security updates

Five years of security updates (from launch date) is provided as an industry standard on premium price-tier phones, which all six tested phones are. Google is the only brand to exceed this, promising seven years of updates. Samsung, OPPO OnePlus, and Xiaomi all provide five years of security updates on the tested devices. That said, documentation on the topic from both Xiaomi and OnePlus is unclear. Xiaomi does not yet have a policy online specifically for the Xiaomi 13, and OnePlus's policy for all consumer devices is not clear online, although it is for enterprise users.

The frequency of updates on Android-based devices (Samsung, Xiaomi, and OnePlus) is dependent on Android, and are therefore the same monthly security patches released by Google. These Android-based devices also benefit from many sensitive aspects being independently updated.

Apple does not give information on the length of support for devices upon release. But there is information on previous devices, which historically show six years or five major operating system updates (as was the case for the iPhone X, released in 2017, which just lost support). Some previous devices have received longer support. Apple is also known to release security-specific updates for unsupported versions when serious issues occur. As of iOS 16, Apple release rapid security response updates separately to operating system updates, expediting the patching of any high-risk vulnerabilities. It could be assumed that Apple will provide the iPhone 15 with five–six years of support, but major device manufacturers should be transparent and open with how long they will support security updates. This is a key theme in product security legislation, regulation, and standards; one example being the UK's Product Security and Telecommunications Infrastructure (PSTI) Act, which will mandate that the manufacturer states the support period for IoT connected devices at the point of sale from 2024.

Huawei does not explicitly document security updates for the P60 Pro. The online bulletin about security updates has not been updated and so only includes the P50 from 2021. In the case of the P50, the documentation does not guarantee any regularity, or lifetime, of updates. Although the P60 is an Android-based device, Huawei does not use Google services, and so extraneous updates via Google Play Services are also not included. Security awareness and remediation

All the Android devices had a similar centralized security and privacy management view in the settings app. This notes the phone configuration, account, lock screen security, and installed app permissions. All also automatically revoked permissions for unused apps.

Even without Google Play Protect, Huawei has implemented similar features on the P60, which gives a detailed summary of recent events and highlights issues for remediation. It also revokes permissions of unused apps.

However, Apple's iPhone 15 does not have such an overview of security settings. Instead, they are spread across multiple areas, such as Lock Screen, Apple account options, and other submenus. There is a Safety Check feature under Privacy & Security within the iPhone settings app, but this menu is mainly for permissions management and the Safety Check feature is only for reviewing and disconnecting an Apple account from other devices and services. iOS does not automatically revoke permissions from unused apps, which means users have to manually remove each permission if needed.

Secure backups

Backup features on the devices tested varied quite largely, although all were end-to-end encrypted. Google's implementation was often stronger than the manufacturer-specific software from Samsung and Xiaomi, respectively.

The Google Pixel 8 backup is inaccessible to Google and is encrypted with the device's passcode. The only exceptions are cloud-based services such as Gmail and Google Photos.

The Samsung Galaxy S23 can be backed up on Google's system or Samsung's own. The latter is encrypted with "enhanced data protection"—meaning normal backups are not encrypted but call logs, messages, apps, settings, and more are encrypted with a user-stored key. Some data, such as attachments, may not be end-to-end encrypted if they are too large.

The OnePlus 11 5G did not have its own manufacturer-made backup option but used Google's backup system—giving the exact same experience as the Pixel 8.

The Xiaomi 13 offered a manufacturer-specific backup solution to the Xiaomi Cloud, which is encrypted but did not specify exact security details or the ability to enable end-to-end backups. For photos, users are directed to use Google Photos.

The iPhone 15 can be backed up via a PC or Mac, or through iCloud. This enables end-to-end encryption by default for passwords, messages, home data, and health data. Apple recently introduced more features, which include end-to-end encryption via the Advanced Data Protection option, but it is not enabled by default. The key is held only on trusted devices and is inaccessible to Apple.

The Huawei P60 lacks access to Google's system and does not offer its own alternative either. Instead, users must do local backups and encrypt them on their PC by using the Hisuite tool. No other option was available on the device, and it is not known what encryption is used on the desktop application.

Physical access control

All phones offer the same biometric access apart from the iPhone 15, which only offers Face ID. The Samsung Galaxy S23 differs slightly by offering an ultrasonic sensor over an optical sensor for fingerprint detection—ultrasonic sensors are in theory better because optical sensors cannot sense depth and are therefore more likely to be tricked —but this was not within the scope of this testing.

iPhone 15's Face ID uses an array of infrared and depth sensors to accurately detect a real face. The Android face unlock available on the tested devices lacks the same sensors and is, in theory, more likely to be spoofed.

All devices except the Xiaomi 13 either required a strong passcode (six or more digits) or issued a warning against using a weak passcode (for example, 111111 or only four digits). And all but the Xiaomi 13 and OnePlus 11 5G offered a lockdown mode to disable biometric entry.

All phones also reverted to requiring a passcode after repeated biometric authentication failures, and then locked the phones following repeated incorrect passcode entries.

Parental control

All Android devices except the Huawei P60 use Google's Family Link. As such the Samsung Galaxy S23, OnePlus 11 5G, and Xiaomi 13 all behave in the same way as the Google Pixel 8. This allows for parents to control the policies of a child's account locally through either the parents' account, the Family Link website, or an app on another device. All policies are included that should be expected, such as blocking certain apps, local features, and services.

Because Huawei does not use Google services, the device has its own offering called Digital Balance, which is limited in comparison: it offers settings to limit screen time and access to apps, but is only available on the device via a passcode-protected page and cannot be managed from elsewhere.

Apple's Family Sharing and Screen Time is similar to Google's offering, allowing the setting up of an account for a parent and associated child to manage policies on the device and remotely.

Consumer perception survey

Background on the survey

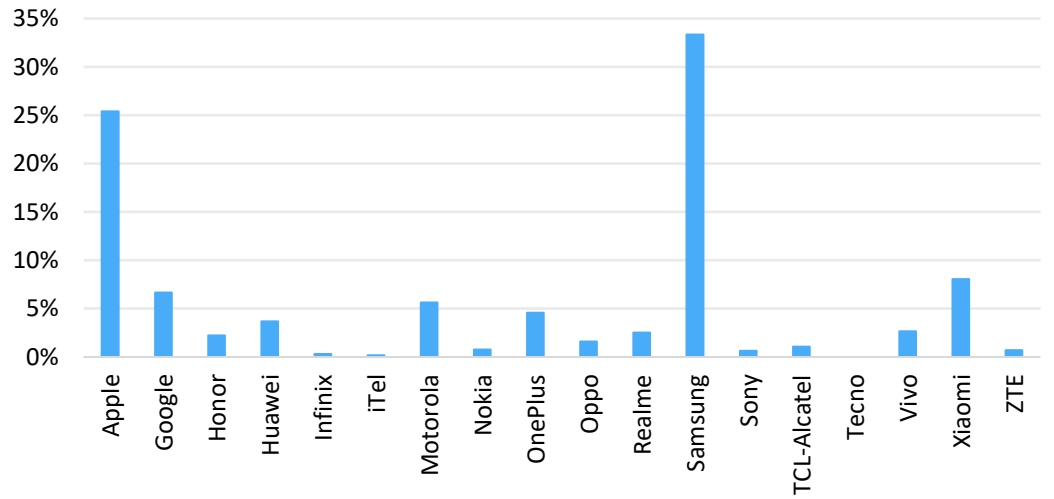
In September 2023, we asked 1,578 people who had bought a new smartphone in the past three years about their security concerns and perceptions in a computer-aided telephone interviews (CATI) survey. People were from the following countries and territories: Australia, Canada, China, France, Germany, India, Ireland, Japan, Singapore, Spain, Taiwan, the UK, and the US.

Key questions asked included, which smartphone brand do you own?, how long did you use your previous phone before upgrading?, and how long do you expect to use your current phone? We also asked them to rate how troubled they were by the 12 security concerns listed in **Table 2**, as well as how effective they think their phone is at protecting them from each.

Key consumer demographics

Smartphone users of 17 different brands were surveyed, with most owning either a Samsung or Apple smartphone. Google, Xiaomi, and Motorola also saw ownership levels of more than 5%, with OnePlus and Huawei also seeing 5% and 4% ownership, respectively. One of the only major smartphone brands not captured in the survey was Tecno, which is a part of Transsion Holdings parent company, although Transsion's other brands iTel and Infinix were included.

Figure 2: Which brand of smartphone do you currently own?

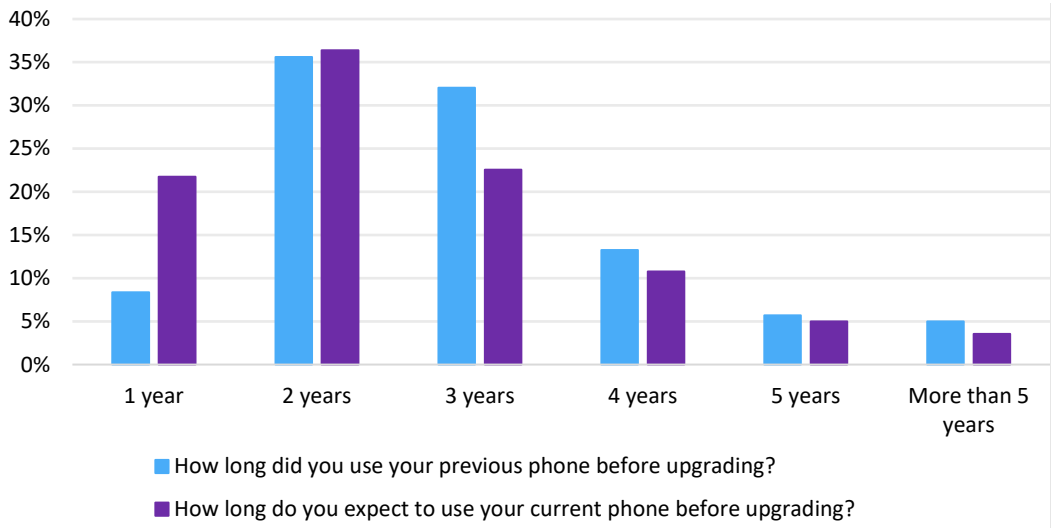


Source: Omdia

With discussion around security update periods being hot in the cybersecurity space, and replacement cycle rates frequently being a sustainability topic, we asked consumers how long they had had their previous phone and how much longer they intend to have their current phone.

With security updates for many phones only lasting two years, a worrying 56% of consumers used their previous phone for longer than this. Just over 5% of consumers reported that they kept their previous phone longer than five years, beyond the security updates of any phone that would have been available at the time. Currently the only phones to offer more than five years of guaranteed security updates are the Google Pixel 8 and 8 Pro, which offers seven years, and the Fairphone 5, which offers eight years.

Figure 3: Consumer smartphone replacement cycle



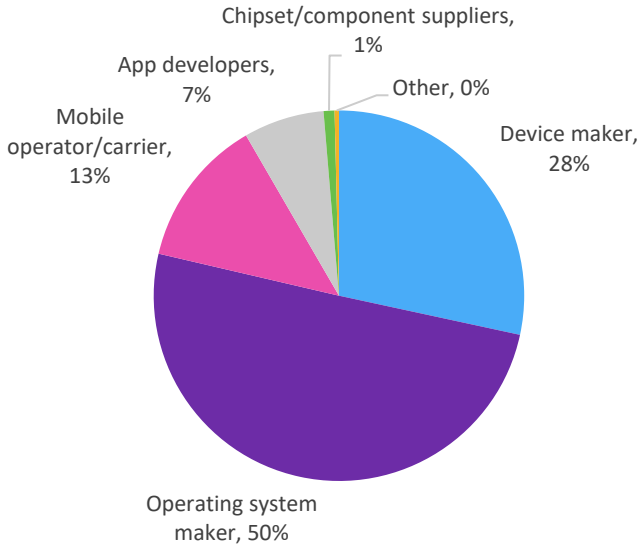
Source: Omdia

Consumer security perceptions

Despite security updates being primarily reliant on the device maker and chipset supplier, most consumers (50%) believe it should be the operating system developer (either Apple or Google) that is responsible for the security of their smartphone.

The mobile operator/carrier should be responsible according to 13% of consumers, showing that perhaps device makers and operators need to do more work together to educate the public on security issues.

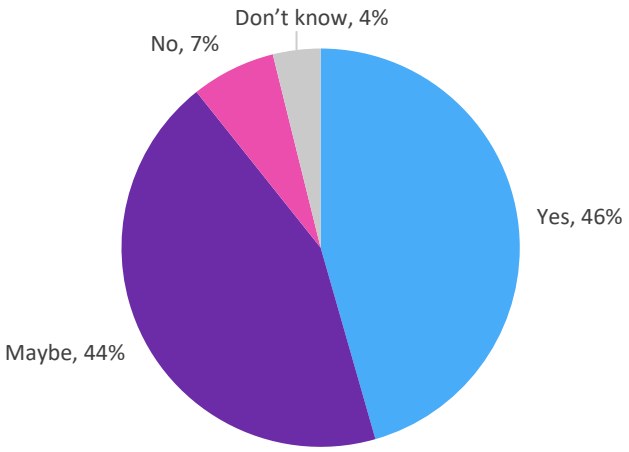
Figure 4: Who do you think is most responsible for security on smartphones?



Source: Omdia

When asked if better security features would be a purchase driver when next buying a phone, 46% confirmed it would be, 44% said it might be, while just 7% said no. The reason for this could be a lack of understanding of security issues, or competing priorities, such as value for money, sustainability, battery life, and so on. Although 69% of respondents thought good security features were critical or important when deciding which smartphone to purchase, respondents were more concerned with long battery life, durability, and processor speed.

Figure 5: Will better security features be a key purchase driver when buying your next phone?



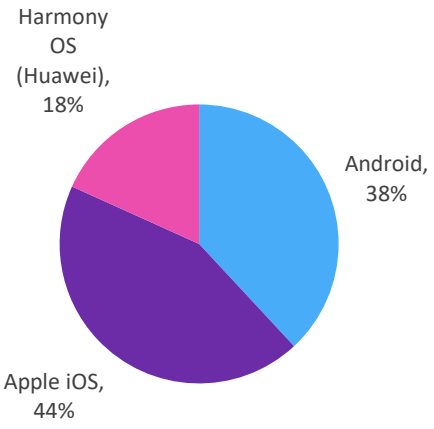
Source: Omdia

When asked to rank the three core operating systems tested in in this report, Apple iOS was rated the most often as being the most secure, closely followed by Android—despite our device testing showing that the Google Pixel 8 Pro (which uses stock Android 14) is more secure than the iPhone 15 (with iOS 17).

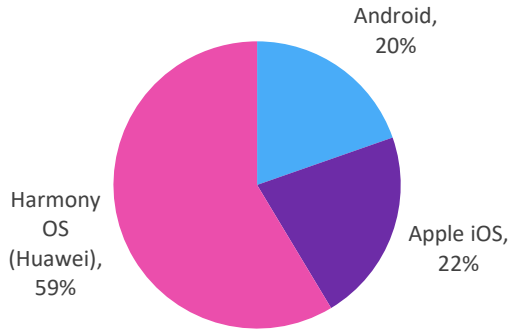
HarmonyOS from Huawei was rated by most consumers as the least secure operating system. The US sanctions against the company could be to blame for this public distrust of the brand.

Figure 6: Which operating system do you think is the most/least secure?

Rated most secure



Rated least secure



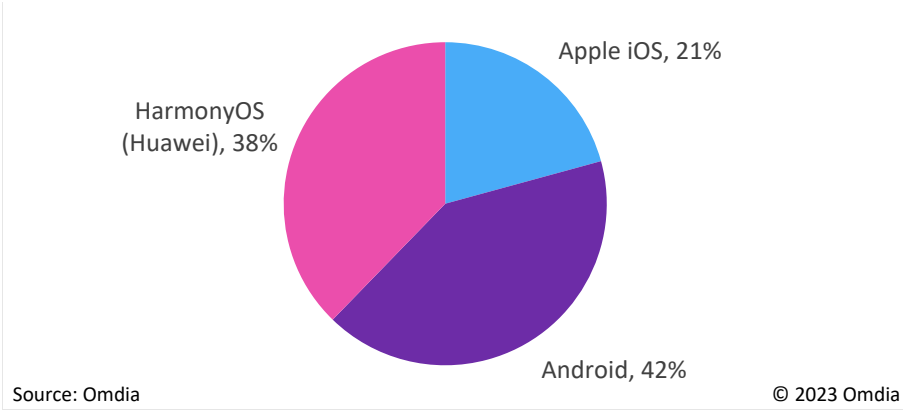
Source: Omdia

Differences by geography

Chinese consumers less worried by security concerns

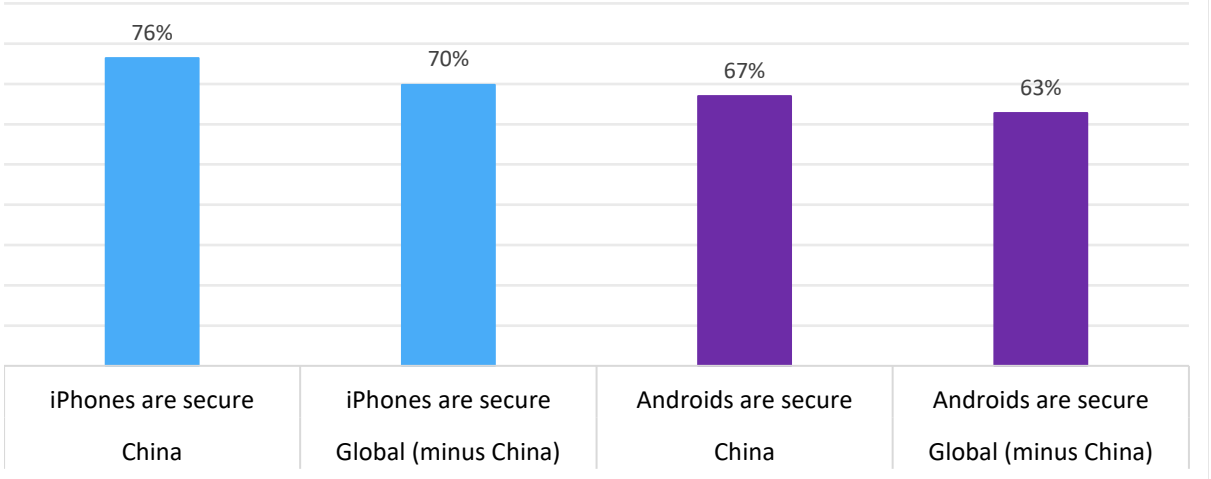
More than the rest of the world, Chinese consumers on average see Android as the least secure and iOS as the most secure of the operating systems. Despite this, Chinese consumers in our survey still agreed that Android smartphones are secure 67% the time, compared to 63% of the time for consumers outside of China. This suggests that although Chinese consumers see iOS as more secure, they in fact see all operating systems as being more secure than do other consumers around the world.

Figure 7: Which operating system do you think is the least secure? (Chinese respondents)



Source: Omdia

Figure 8: Net agree ("strongly agree" and "agree") with the following statements



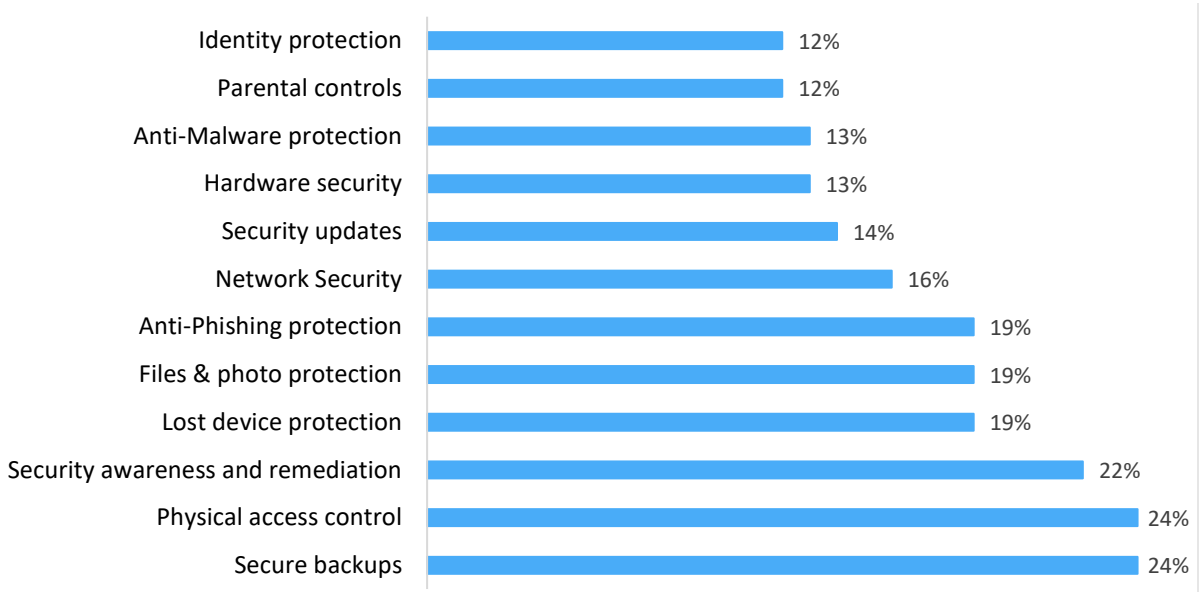
Source: Omdia

Indian consumers most likely to say their smartphone is not effective at addressing security concerns

While Chinese consumers are most likely to trust their devices' effectiveness, Indian consumers are the most skeptical. When asked to rate how effective their phone is at addressing the 12 security concerns in our test, on average 17% of Indians said they thought their phone would not be effective.

This level of distrust is worst for secure backups and physical access control, meaning that almost one in four Indian smartphone consumers do not believe their devices' backups are safe or that their smartphones can prevent people from breaking through their lock-screen biometrics or passcode.

Figure 9: How effective is your smartphone at addressing the following issues? Percentage who answered "not effective" (Indian respondents)



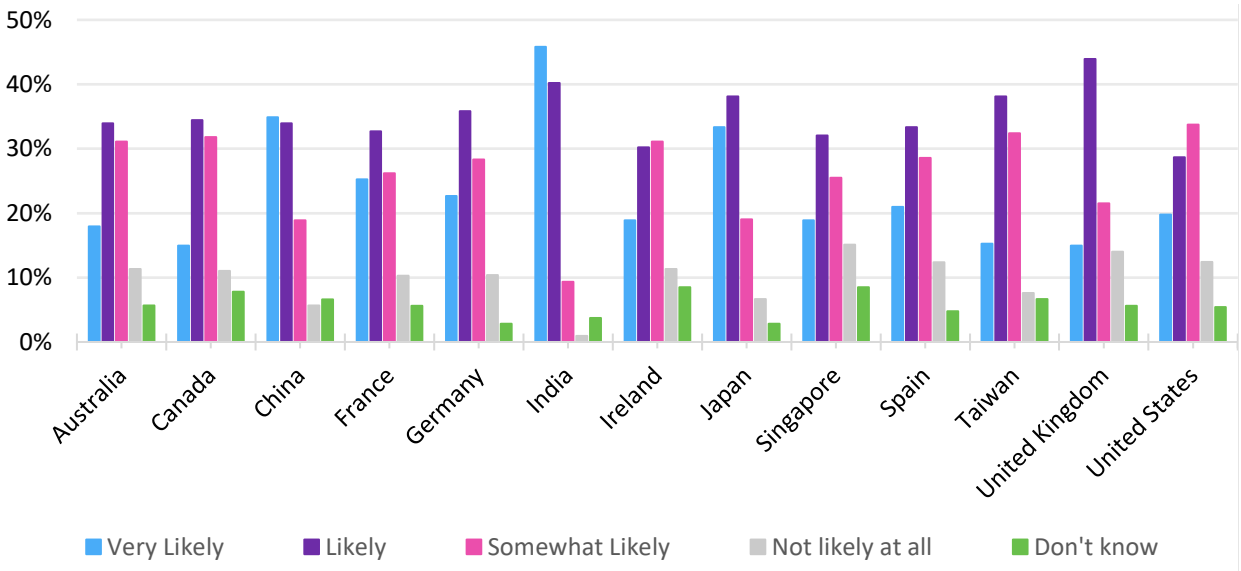
Source: Omdia

Indian smartphone users most likely to pay more for a phone with security features

Almost half of Indian respondents to our survey reported that they were “very likely” to pay a premium for a phone with advanced built-in security features. This is quite different to Canada or Taiwan, where only 15% said the same, or the UK, where 14% said they are “not likely at all” to pay a premium.

This likely comes from both the increased concern for security risks in India and the belief in other countries that advanced security features should be built into phones as standard and not at extra cost.

Figure 10: How likely are you to pay a premium for your next smartphone to have it equipped with advanced built-in security features?



Source: Omdia

Authors

Aaron West
Senior Analyst, Smartphones
aaron.west@informa.com

Hollie Hennessy
Senior Analyst, Cybersecurity
hollie.hennessy@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer