Publication date:
October 10, 2022

Author:
Hollie Hennessy

Mobile Device Security 2022

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

Brought to you by Informa Tech

Contents

Summary

Google’s Pixel 7 tops security ratings for features consumers rate as most important

Google’s Pixel 7 scored ahead of Apple’s iPhone 14 and Samsung’s Galaxy S22 in Omdia’s annual Mobile Device Security Buyers’ Scorecard. Apple’s iPhone 14 topped Samsung’s Galaxy S22 which was ahead of Xiaomi.

The ratings were based on hands-on testing by Pen Test Partners, combined with importance ratings from a survey of 1,500 consumers across eight major countries in the Americas, Asia & Oceania, and Europe.

Table 1: The four leading smartphones rated on their security features

Feature	Consumer importance weighting	Ideal score	Google Pixel 7	Apple iPhone 14 Pro	Samsung Galaxy S22	Xiaomi 12
Identity protection	1.0	9.0	9.0	7.0	5.0	0.0
Security updates	0.9	3.6	3.2	3.6	3.4	3.0
Network security	0.8	2.4	2.0	1.2	2.0	0.4
Secure backups	0.7	1.4	1.4	0.7	0.0	0.7
Hardware security	0.6	1.2	1.2	0.6	0.6	0.6
Anti-malware protection	0.5	1.0	1.0	0.5	1.0	1.0
Physical access control	0.4	1.2	1.2	1.2	1.2	0.8
Anti-phishing protection	0.3	1.8	1.2	0.0	0.9	1.2
Lost device protection	0.2	2.0	1.6	1.6	1.8	1.8
Total		**23.8**	**21.8**	**16.4**	**15.9**	**9.5**

Source: Omdia © 2022 Omdia

Key findings

While Google's Pixel 7 scored well overall, each smartphone lacked some features. For example, no devices could prevent new manually crafted phishing attacks. However, Android devices could prevent users from accessing phishing pages deployed with common social engineering tools owing to the system's extensive use of Google Safe Browsing.

While you can sideload on both iOS and Android platforms through different means, the Android system warns the user about sideloading external applications in their system. The user could still install applications outside the Google Play store by design where on iOS there is more of a loophole using enterprise developer certificates.

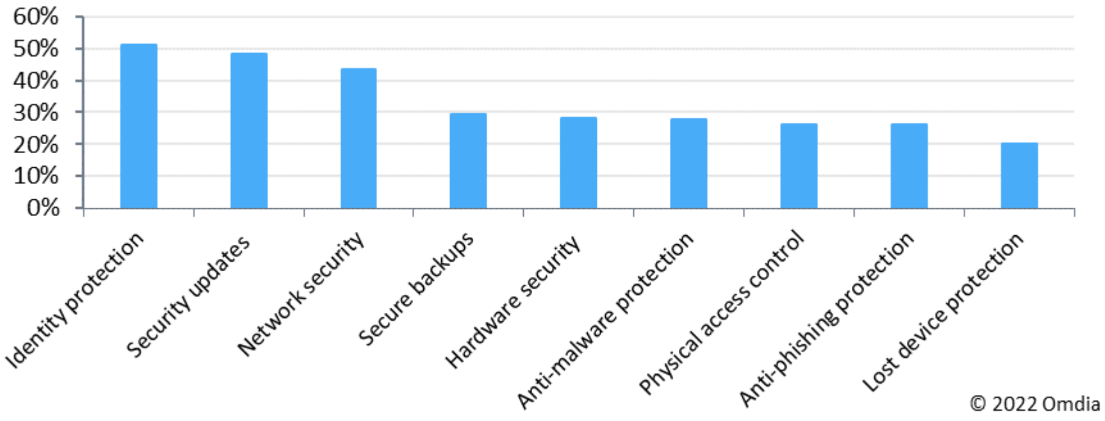
The iPhone 14 Pro devices sold in the US do not use physical SIM cards. This improves security by making it harder to disable network connections if a device is stolen.

On identity protection (the most important feature to users), all phones offered strong two-factor authentication options for main accounts. Secondary accounts were also assessed; Xiaomi lacked two-factor authentication on the account tested.

In the physical access control category, all devices had satisfactory implementation, including biometrics. However, the iPhone 14 Pro did not have a fingerprint reader and relied on face scans.

In the iPhone's iOS 16, Apple introduced the "lockdown" mode to mitigate sophisticated attacks against targeted individuals. This feature disables many of the phone's functionalities and is not intended for standard users; therefore, it was not included in the test.

Figure 1: Security features most important to consumers



Notes: n=1,500; multiple respondents allowed.

Source: Omdia

Consumers rated identity protection as their most important security concern, closely followed by security updates and network security. Each respondent was asked to select their most and least important smartphone security concerns from a list provided in a computer-aided telephone interviews (CATI) survey. The respondents were qualified by screening questions that they were familiar with smartphones acquired within the last three years. Definitions of the security feature criteria in this survey and hand on tests were as follows:

Table 1: Security features covered in Omdia's consumer survey

Feature	Description
Anti-malware protection	A set of tools to detect and block software designed to disrupt, damage, or gain unauthorized access to a smartphone and the data that resides on it.
Anti-phishing protection	A set of tools to help stop bad actors from using fraudulent emails, texts, or phone calls to trick individuals into revealing personal information, such as passwords and credit card numbers.
Hardware security	Using a smartphone's hardware to offer higher levels of protection for sensitive data that resides on a device.
Security updates	A security update to fix issues in a smartphone's software that bad actors could use to corrupt a device or steal information from it.
Network security	The ability to protect a smartphone's communications to various cloud services and its internet connection overall. Network security ensures that data transfers over the internet are not intercepted or spied on.
Identity protection	A set of tools to help generate and store passwords securely for all apps and websites. Identity protection also proactively notifies a user if any previously used passwords have been leaked or stolen so the user can immediately change their password. In addition, multiple factors (something you know and something you have) can be leveraged for identity protection.
Physical access control	The ability to prevent bad actors from gaining unauthorized access to a device by either presenting an artificial copy of a user's fingerprint or by trying to repeatedly guess their passcode.
Lost device protection	The ability to locate, track, lock, or even remotely wipe a lost or stolen device using a website or another device, such as a family member's or friend's smartphone, computer, or tablet.
Secure backups	The data backed up from a user's device is protected (using encryption) while it is transmitted to various cloud services. This data is also protected while residing in the cloud service.

Source: Omdia © 2022 Omdia

Test results

Identity protection

The Google Account offered more options for two-factor authentication and implemented a satisfactory audit trail of account activity in its user interface; however, two-factor authentication had to be manually enabled on the test account. Android devices benefit from Google's two-factor authentication options for main accounts. Meanwhile, the Galaxy S22 and Xiaomi 12 devices use secondary accounts to access manufacturers' specific features. Samsung accounts offered strong two-factor authentication options, while Xiaomi accounts offered weaker authentication methods without two-factor authentication support. Compared to Google accounts, which supported all features tested, Apple accounts offered strong two-factor authentication options; however, they lacked an audit trail of account logins and the support of physical security keys.

Security updates

Google's Android version updates have been labeled by patch level, with patch launch dates corresponding to the Android system's security level. Android phones receive security updates very often; Google makes available monthly updates of the Android Open Source Project (AOSP). With the modularization of Google's operating system in recent years, security updates are delivered much faster and more regularly than before; parts of the Android system (such as the Google Play Services and Google Chrome and WebView) are directly updated by Google.

Both iOS and Android systems had strong updating capabilities and responses to online security threats. The modularization of the Android operating system and the new "Security Responses & System Files" feature enable security updates to be pushed to users' devices even faster.

When looking at the support period of previous Apple's flagship iPhone models, it was observed that these received, on average, six OS updates. Therefore, it is expected the iPhone 14 Pro to be supported for the same time as its predecessors. iOS major releases are launched every year. Security updates were seen to be released every month or so, and Apple sometimes provides security patches for unsupported iOS versions for serious vulnerabilities. iOS 16 comes with the "Security responses & System files" feature, which allows automatic installation of patches on the phone to mitigate security threats.

Network security

The Pixel 7 and Galaxy S22 had the option to disable 2G networks; however, to achieve this on the Galaxy S22, the user cannot use 5G or LTE networks.

Web traffic can be observed on all devices if a proxy is configured, allowing interception of unencrypted traffic. To intercept encrypted data (which constitutes most smartphone data), it is necessary to manually install a CA certificate onto the device. Furthermore, many apps implement certificate pinning, which can only be defeated with a rooted or jailbroken device or using advanced techniques. On iOS this is still possible by installing a certificate and trusting it. On Android this is not possible out of the box, even if a user installs the certificate apps do not trust that certificate.

The iPhone 14, Pixel 7, and Galaxy S22 support eSIM for authentication by mobile providers. On October 4, Xiaomi announced that the Xiaomi 12T will have eSIM support. The announcement came after the evaluation and therefore was not included in the score.

Secure backups

Apple encrypts users' backups while in transit and stored on its servers but does not offer end-to-end encryption. Google offers end-to-end encrypted backups; however, not all of a user's data stored on Google servers is end-to-end encrypted. Samsung does not provide information on how backups are stored on its service, while Xiaomi offers encrypted backups of limited applications and users' data.

Hardware security

It is challenging to compare the hardware security of different platforms because they interface with different software using different methodologies. Although all Android phones supported TrustZone (a trusted execution environment running on the AP), the Google Pixel 7 was seen to have an enhanced security hardware design compared to other Android devices, given its additional layers of hardware, such as Tensor core and Titan M2 chip.

Hardware security for the other phones evaluated was also proven to be effective. For example, the iPhone's security modules, with the Secure Enclave coprocessor, were successful in protecting users' data.

Anti-malware

Android-based phones allowed application sideloading by offering on-screen exemptions to security warnings and letting the user decide whether to install the application. Xiaomi scanned the sideloaded application, correctly flagging it as a virus and displaying a warning that could be bypassed. iOS allowed sideloading by means of stolen developer certificates.

Google Play Protect, which came bundled in all the Android models tested, was ineffective in detecting newly crafted malicious applications that were sideloaded on the phones. However, once Play Protect scanned the malicious app, it warned the user about the threat, even when the application had been installed on other Android devices.

Physical access control

Apple does not provide fingerprint recognition on the iPhone 14 Pro, but its Face ID outperforms competitors by offering the most advanced face scan system. However, the face scan method could be considered less secure because people with similar facial features (such as siblings or twins) could unlock devices; this does not affect security for most users. The Pixel 7 offered all forms of biometric verification tested. The statistical probability is higher—and further increased if using Face ID with a mask—for twins and siblings that look like you, and among children under the age of 13, because their distinct facial features might not have fully developed. Using a passcode to authenticate is recommended. All phones had a method to disable biometrics quickly, except the Xiaomi 12.

Anti-phishing

No devices detected or blocked the manually crafted phishing page and SMS messages. Android devices successfully blocked users from navigating to phishing sites created with known tools and warned users via the Gmail app. This success was due to Google Safe Browsing, a service that provides updated lists of web resources containing phishing content or malware. When websites are viewed on Google applications, they are scanned for malicious patterns and added to the Google Safe Browsing list. This list is also used by other browsers, such as Safari and Firefox. Apple proxies Safe Browsing in Safari through its servers instead of querying the list directly from Google; this could explain why Safari did not warn the user when the phishing website had already been flagged as malicious on Android phones. Messages received on WhatsApp were also successfully blocked by Google Chrome once opened.

The Pixel 7 and Xiaomi 12 were the only phones in the assessment with native call ID and spam protection implemented.

Lost devices

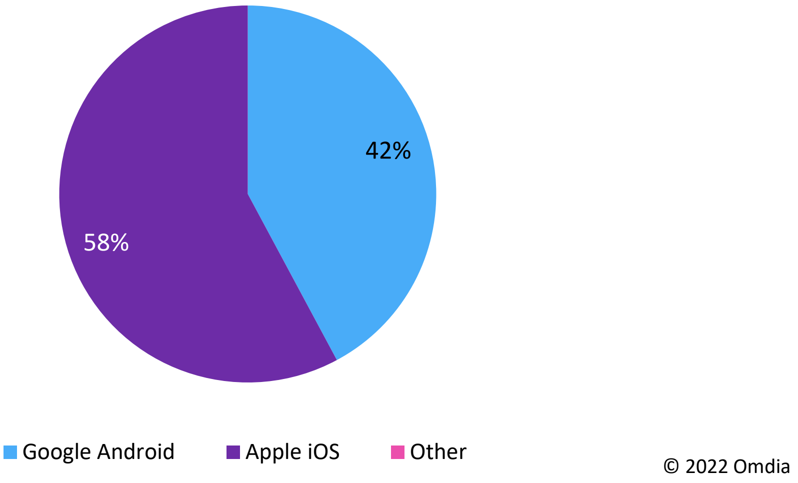
The iPhone 14 offered satisfactory options for finding, locking, and tracking devices. All three Android devices tested allowed users to see notifications and SMS messages while locked, using Google’s Find My Device service with the devices’ default configurations. This feature is concerning because an attacker could request two-factor authentication messages to the phone to access other services.

Samsung and Xiaomi offered enhanced finding options, sometimes exceeding Apple’s finding capabilities, but only for users with additional accounts. Xiaomi users could also manually configure their devices to be able to use their finding service.

Consumer perceptions

Although Android devices (such as Google’s Pixel 7 and Samsung’s Galaxy S22) scored higher on consumers’ most important security features, smartphone buyers still perceive Apple’s iOS as more secure than Android, as shown in Figure 2.

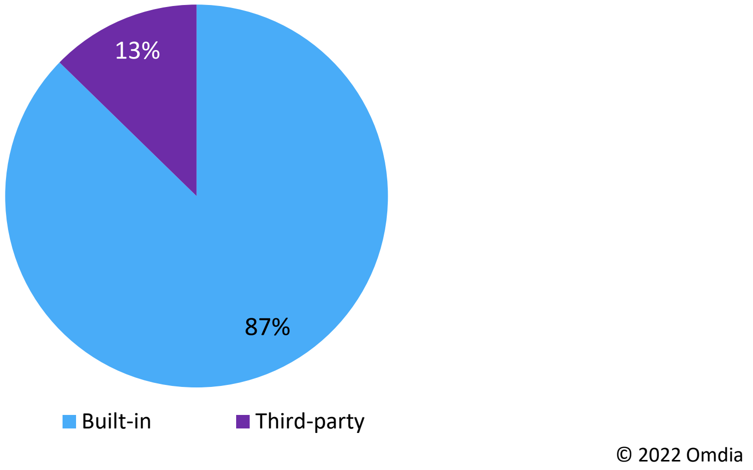
Figure 2: Consumer perceptions on the most secure operating system



Source: Omdia

Consumers also overwhelmingly want security features built into their smartphones rather than purchasing them from third parties, as shown in Figure 3.

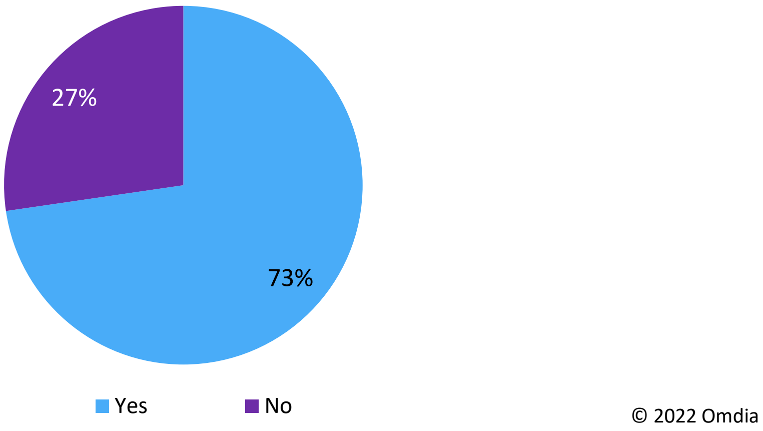
Figure 3: Consumer preferences on built-in security features in smartphones vs. purchasing from third parties



Source: Omdia

Most consumers would pay a premium for a phone with all the security features built-in, as shown in Figure 4.

Figure 4. Consumers' willingness to pay a premium for a phone with all security features built in



Source: Omdia

Author

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

Mike Sullivan-Trainor
Director, Consulting, Cybersecurity
Mike.sullivan-trainor@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia research and 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

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.