Publication date:
October 2021
Author:
Mike Sullivan-Trainor
Hollie Hennessy
Gerrit Schneemann

Omdia Consumer Mobile Security Scorecard

Pixel 6 garners top score for smartphone security; users see identity protection as most important issue

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Google

Contents

Summary

In 2020 Omdia launched its first Mobile Security Scorecard, assessing the security concerns of enterprises through a survey of 700 enterprise decision makers. In September 2021, to complete our evaluation of mobile device security, we surveyed 1,520 consumers of smartphones (priced $200 and up) across 10 countries to determine their assessment of the most important security features. These results were coupled with a hands-on evaluation, conducted by Omdia's analyst team, of four leading smartphones, including the latest available models and operating systems, from Apple, Google, Samsung, and Xiaomi.

The Consumer Mobile Security Scorecard found that Google Pixel 6 had a perfect score for all the hands-on evaluation categories with the highest ratings for security features (a weighted score of 5.4), well ahead of the other devices, while Samsung's Galaxy S21 Ultra performed second best (4.4 weighted score), and Apple's iPhone 12 Pro and Xiaomi's Mi 11 5G were virtually tied (4.03 and 4.05 weighted score respectively). Apple's iPhone 13 was not available at the time of the evaluation; however, the score would not have changed.

In summary, mobile device suppliers, led by Google, appear to be largely addressing consumers' smartphone security concerns with a variety of tools and features. If anything, there is a continued need for smartphone OEMs and wireless carriers to educate users on the potential threats and existing features to combat these threats. Key to this is making security features a focus of the user interface instead of hiding many of them in settings menus.

Methodology

The Consumer Mobile Device Security Scorecard was developed using a two-part approach. First, a consumer survey was conducted to determine the importance of security features to smartphone users across all phone brands but focusing on users with handsets priced at $200 or more. Respondents were from the following countries: Australia, Canada, France, Germany, Ireland, Japan, Taiwan, the UK, and the US. The respondent group included all age brackets from 20 to over 60 and all genders.

Second, a hands-on test was conducted by Omdia experts in mobile devices and cybersecurity for the items that could be tested. A test protocol was determined for each security feature, designed to replicate a consumer's ability to use the security tools provided by each manufacturer or the availability of security measures built into the hardware or software of the device. The phones were tested "out of the box" with no additional software or advanced configuration applied.

The scoring was based on the hands-on test, which included a rating of 0 to 1 for each feature for each phone, with 1 being very good (i.e., providing a full set of tools to address the feature) and 0 meaning no tools. The weighted scores were calculated by multiplying the test scores by a relative importance rating from 0.2 to 1, assigned based on importance from the consumer survey.

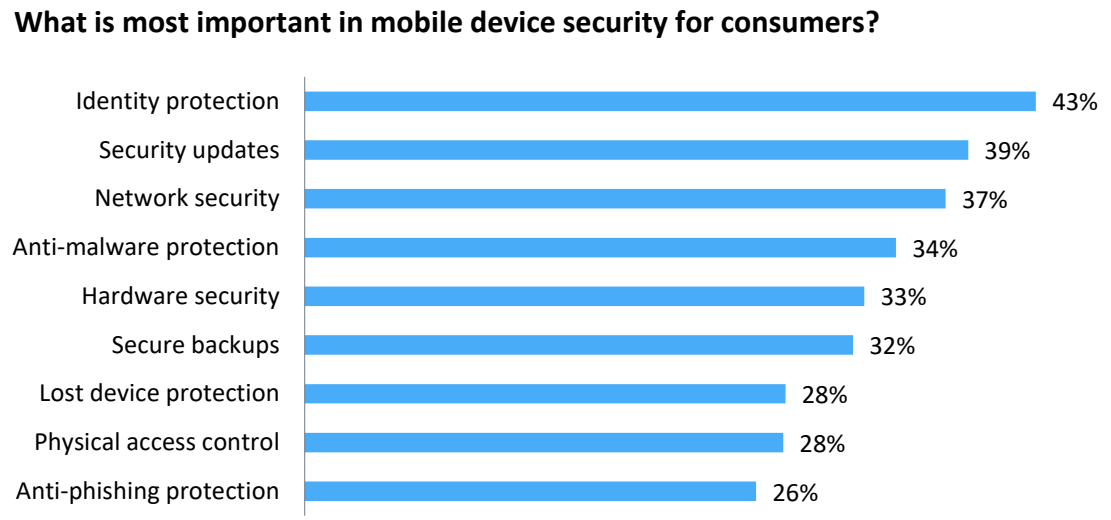
Figure 1: Mobile device security, buyers' scorecard

	Brand	Apple	Google	Samsung	Xiaomi
	Phone type	iPhone 12 Pro	Pixel 6	Galaxy S21 Ultra	Mi 11 5G
	Operating system	iOS 15	Android 12	One UI 4.0, Android 12	MIUI 12.5
Feature	**Weighting**	**Score**	**Score**	**Score**	**Score**
Anti-phishing	0.2				
Anti-malware	0.7				
Security updates	0.9				
Hardware security	0.6				
Network security	0.8				
Identity protection	1				
Physical access control	0.3				
Lock/locate/track lost device	0.4				
Secure backups	0.5				
WEIGHTED SCORES	**5.4**	**4.03**	**5.4**	**4.4**	**4.05**

Source: Omdia

Evaluation results

Figure 2: Consumers' top mobile device security priorities



Note: n=1,520

Source: Omdia

Identity protection

Identity protection was identified as the most important, most in-demand feature, which is likely driven by the increased data breaches and malicious actors attempting to steal digital identities. All the devices evaluated provided some form of step-up verification. For Apple this was limited to one-time passwords (OTP), while Google supports OTP, push notifications, and physical and phone-based FIDO security keys. Xiaomi and Samsung devices also asked the end user to register accounts with their respective backends, and those accounts only supported OTP, which resulted in a lower score for them. Other criteria evaluated for this category include built-in support for password management (i.e., password generation, usage, and checking for compromise) and any kind of proactive check-up features, account monitoring, and alerting. While Pixel 6 scored highest in this category, all phones fared well with a 0.75 weighted score.

Security updates

All suppliers except Apple list the security update support period for their devices. For the Google Pixel 6, Google commits to a solid five years' security update period for consumers from launch, the longest support period offered for the four devices. While our survey suggested most respondents like to have the latest device or only keep their device for a couple of years, security updates are necessary for those who do not and for the secondhand smartphone market. Having a defined period is necessary for consumers to know about the security support they will receive if they are purchasing a new or used mobile.

Samsung offers a minimum of four years' firmware updates for the Samsung Galaxy S21 Ultra. While Xiaomi promises a minimum of two years for all devices in general and four for its newer devices, there is no exact time period for the Mi 11 5G in its documentation. Apple devices tend to receive around five to six years of support; however there is no documentation guaranteeing this or defining any support period for consumers.

Upfront commitment and longevity of security updates was part of the criteria, the other part was evaluating how security updates work on the various devices/operating systems. While on iOS security updates get pushed down as part of a larger update, on Android these updates actually get distributed through multiple mechanisms such as dedicated security updates which are separate from feature updates. There are also Google Play System Updates which launched with Android 10 and have been expanding. Lastly, Android apps for things like dialing phone numbers, sending and receiving text messages, and the web browser are all updated directly through Google Play as opposed to having to be updated through a monolithic update. This provides much better agility when it comes to pushing out critical security updates for those items.

Network security

It is possible to see device data in transit from both the web and third-party applications on Apple iPhones. However, since Android 7, third-party apps on Android devices have secure connections that trust preinstalled certificates only. This means a user cannot be fooled into installing a malicious certificate that could expose all their device or app traffic.

The Google Pixel is the only device that gives the user the option to disable 2G, which is known to have more security vulnerabilities than later mobile generations.

Hardware security

All the phones rely on some form of hardware-based security capabilities. All modern Android devices use a Trusted Execution Environment (TEE). This is designed to isolate from the rest of the device's operating system, protecting the most sensitive data inside.

Apple's device does not have this built in, but it does have the Secure Enclave Processor, which protects and stores particularly sensitive information. The Qualcomm SoC powering the Xiaomi Mi

11 5G appears to have a similar feature with its Qualcomm secure processing unit (SPU). Samsung similarly has a secure processor and memory, branded Knox Vault, with the S21 Ultra.

Google's Pixel 6 is the only device Omdia looked at with a third layer of security, combining its new Tensor security core with the Titan M2 Chip and a TEE.

Anti-malware

Although it is difficult, especially with iOS, it is possible to sideload an application onto all devices outside of the dedicated app store. In all cases, however, the user is prompted with many warnings along the way. While Samsung, Google, and Xiaomi have anti-malware solutions built into their devices to protect and detect malicious software, Apple is lacking here.

Secure backups

Only Google's Pixel 6 has end-to-end encryption of data backed up to the cloud. Data is encrypted in transit and in storage; no one can access and decode it, not even Google. With Xiaomi and Apple devices, there are some levels of encryption (such as health and other important data being encrypted end to end with Apple or data being encrypted and safe in transit to the Xiaomi Cloud), but it is not assured that the hosting provider does not have access to any backups. End-to-end encryption for sensitive information is only available with Apple if two-factor authentication is turned on. In contrast, Samsung device backups can have access to login and PIN for the device, meaning data sent to the cloud is not securely end-to-end encrypted.

Lost devices

Each manufacturer has a web-based tool to locate, trigger, lock, and wipe the device should it be lost or stolen. However, only Google and Apple have a dedicated mobile app to do this as well. There is the option to locate via mobile with Xiaomi, but only after Google's Find my Device app has been downloaded separately.

Physical access control

All devices offer some form of biometric access control, whether that is face or fingerprint scanning, which can downgrade to passcode access. Most of the device manufacturers offer an option to temporarily disable biometrics, an additional security measure to protect against being forced to unlock your device. However, Xiaomi's MIUI 12 does not offer this feature.

Anti-phishing

Surprisingly, anti-phishing protection was seen as least important by consumers as a mobile phone security feature. It may be that consumers see this function as more of an email or network security issue than something that can be addressed by the device. However, anti-phishing, which was described as 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, is addressed by the devices.

Overall, many of the current anti-spam or anti-phishing implementations require users to dive deep into the settings of their phones and proactively seek out some of the available features to protect themselves. This is particularly obvious with the Xiaomi device. Despite using Google's messaging app, it requires the user to apply "spam protection," which is off by default. Without it, SMS phishing attempts are not flagged. Similarly, in the Mi Browser, there are no warnings after a phishing link is clicked. However, there is the option to use Chrome as a browser, so while the enhanced anti-phishing protection is not enabled by default, users can enhance their security protection by switching to Google's app.

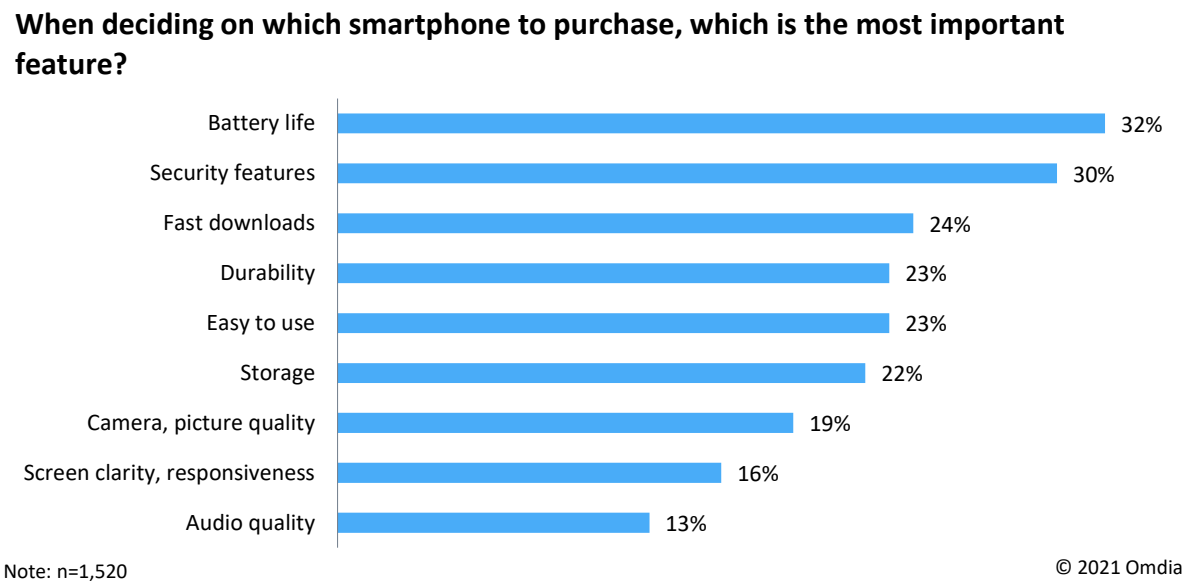
Apple's iPhone 12 detects phishing attempts in its Safari browser. The device has an option to silence unknown voice callers, but call blocking and identification are dependent on the mobile operator. Android phones rely on Google Safe Browsing, which can detect both phishing and malware-based websites. On Android, Google Safe Browsing is used in the Chrome browser, Chrome custom tabs (CCT), and WebView. On Pixel devices running Android 12, there is an additional layer of on-device anti-phishing detection that works in third-party messaging applications: if a suspicious looking message comes, the user is alerted.

Gmail also provides built-in malware/phishing prevention as well as support for Verified Logos using Brand Indicators for Message Identification (BIMI). Caller ID and spam protection automatically flag known scammers and potential voice-based phishing attempts. Spam protection is built in to the messages application. Call screen gives users the ability to screen their calls before deciding whether to pick up the call. Call screen is only available with Google Pixel, and while the other features are available with Android phones, they are not always activated on the device by default: Xiaomi does not have spam protection turned on in the messages app; consumers have to enable it themselves.

Survey results

Relative to other buying decision factors, consumers named security features as the most important, second only to battery life and well ahead of other criteria.

Figure 3: Consumers' most important buying decision criteria

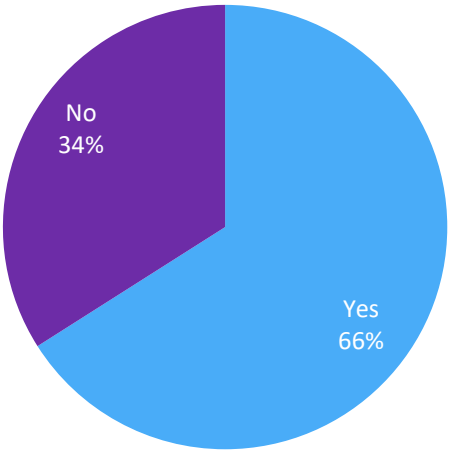


Source: Omdia

In addition, the majority of users report purchasing third-party software for security. However, the vast majority of them would like to see their security issues addressed by the phone suppliers.

Figure 4: Most consumers have bought third-party security software

Have you purchased security software for anti-virus, anti-malware for mobile devices?

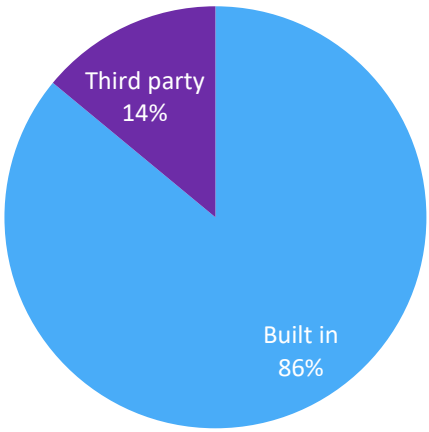


Note: n=1,520

Source: Omdia

Figure 5: Most consumers would prefer security built in

Would you prefer security features to be built in to a smartphone or to purchase third-party security software?



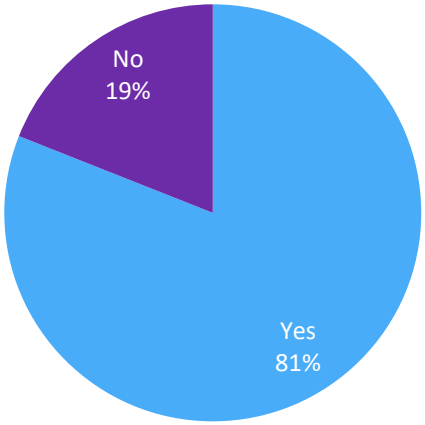
Note: n=1,520

Source: Omdia

The importance of security to consumers was finally underlined by the finding that more than 80% consider security features to be a key purchase driver, and 67% of them would pay a premium to have the security features built in.

Figure 6: Security is a key purchase driver

Would better security features be a key purchase driver when you buy your next phone?

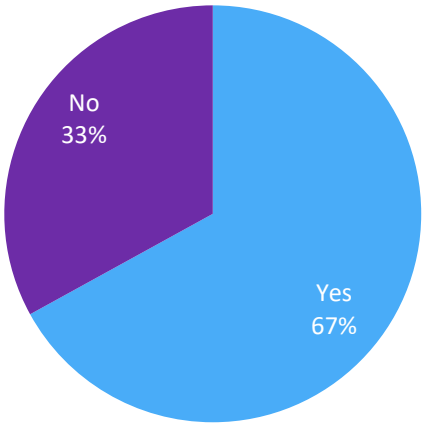


Note: n=1,520

Source: Omdia

Figure 7: Consumers are prepared to pay a premium for security

Would you pay a premium for a phone that had all of these security features built in?



Note: n=1,520

Source: Omdia

The combination of the importance of security and smartphones' current feature compliance, led by Google's Pixel, point to a strengthening landscape for consumers to address security threats.

Enhanced features in future releases along with consumer education will continue to build on this set of capabilities.

Appendix

Methodology

Omdia surveyed 1,520 consumers of smartphones (priced $200 and up) across 10 countries. The respondent group covered all age brackets and genders. To determine scores for each device, a hands-on test was conducted by Omdia experts in mobile devices and cybersecurity.

Scoring was based on the hands-on test, which included a rating of 0 to 1 for each feature for each phone. The final weighted scores were calculated by multiplying the test with a relative importance rating based on importance information gleaned from the consumer survey.

Authors

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

Hollie Hennessy
Senior Analyst, Cybersecurity

Gerrit Schneemann
Principal Analyst, Smartphones

Get in touch

www.omdia.com
customersuccess@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

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.