COMPARISON

GUARDDO PIXEL AND GRAPHENEOS

Independent secure spaces

GRAPHENEOS	GUARDDO PIXEL
The GrapheneOS interface does not conceal the presence of other profiles, which reduces the confidentiality of information. Access to a secure profile in GrapheneOS requires entering the primary space first.	**It has two independent secure spaces. The “gray” space cannot be detected. Each space can be opened directly from the lock screen using a different password or fingerprint.**

Emergency data deletion

GRAPHENEOS	GUARDDO PIXEL
Data can be deleted using a PIN or password.	**Several triggers are supported: a special password or fingerprint, a series of incorrect attempts, a wipe button, inactivity, activation of airplane mode, or an SMS sent to GuardDo Pixel from any phone containing a preset phrase.**

Open source code

GRAPHENEOS	GUARDDO PIXEL
The code is open, but information about updates is not visible.	**The source code is fully open and can be reviewed on GitHub or GitLab. All updates and changes to our devices are also published on the GuardDo website.**

Protection against forensic tools

GRAPHENEOS	GUARDDO PIXEL
The Cellebrite UFED forensic system and Pegasus software pose a threat to GrapheneOS when it is configured incorrectly.	**It is fully protected against interference by third-party forensic tools. The information remains secure, and forensic tools cannot reveal the existence of the second space or the information stored in it.**

Secure connection settings

GRAPHENEOS	GUARDDO PIXEL
It has no built-in VPN or proxy.	**Built-in tools to bypass blocking include two VPN servers, DPI circumvention, a secure proxy for Telegram, and location spoofing with a choice of any city in the world.**

Support and feedback

GRAPHENEOS	GUARDDO PIXEL
Dedicated personal support is not available to customers.	**GuardDo provides direct technical support and feedback from its team, including help with setup, use, troubleshooting, and configuration of individual features.**

SIM card operation

GRAPHENEOS	GUARDDO PIXEL
It has no additional protection.	**Built-in SIM masking hides SIM card data from applications. SIM settings also allow two different SIM cards to be used in two separate spaces.**

Installing applications

GRAPHENEOS	GUARDDO PIXEL
Applications are installed through Sandboxed Google Play, a more secure version of Google Play.	**A proprietary anonymous app store installs familiar Android applications without requiring a Google account, using generated anonymous tokens (random accounts).**

Absence of Google trackers

GRAPHENEOS

Google trackers are absent. However, if you sign in to Google services in one space (using Google fingerprint spoofing), you are automatically signed in in the other space as well.

GUARDDO PIXEL

Google trackers are also absent, but signing in to Google services (using Google fingerprint spoofing) occurs in only one space. The second, “gray” space is not automatically signed in. The spaces remain independent and secure.

Formatting the phone by third parties

GRAPHENEOS

GrapheneOS is vulnerable to device formatting through Recovery Mode.

GUARDDO PIXEL

GuardDo Pixel does not allow access to Recovery Mode to format the phone.

Application checks during installation

GRAPHENEOS

Not available.

GUARDDO PIXEL

Each application is checked during installation by PackageInstaller (the Android app installer), which is built deep into the system level. It also displays the threats and trackers the application contains, helping protect the device from malicious software.

Comparison of code improvements

GRAPHENEOS

It has functional shortcomings in its code that affect the user experience and cause noticeable inconvenience.

GUARDDO PIXEL

Our technical team has done extensive work to make our device as pleasant to use as possible. At the code level, we have developed technical solutions that are absent from GrapheneOS. To avoid overloading this table, here are a few examples:
Code improvements:
Race condition in notifications (fixed)
NPE in TextToSpeechManagerPerUserService (fixed)
QSAnimator crash (fixed)
NPE in SettingsLib for fragments without a divider (fixed)
Crash when changing configuration due to ConcurrentModificationException in SystemUI (fixed)
Secondary user crash when the system user is locked (fixed)
NPE in ArtFastDataOutput.writeUTF() (fixed)
Memory leak in car service (fixed)
FlashlightControllerImpl crash when the camera ID list is empty (fixed)
Screen flicker when launching landscape applications from portrait mode (fixed)
ConcurrentModificationException in LocaleStore (fixed)