

iodé

iodéOS = LineageOS + MicroG + Firewall

April 22, 2022

draft v0.1

Introduction

iodéOS is a privacy-focused operating system powered by LineageOS¹ and based on the Android mobile platform (AOSP²).

The objectives in the conception of iodéOS are threefold:

- To keep the stability and security level of LineageOS, by minimizing the modifications made to the system. Apart in-depth modifications required by the firewall, which operates at the system level, we mainly only changed default settings to prevent data leaks to Google servers.
- To ease a quick adoption by new users. We especially target users that are concerned by the protection of their privacy, but are not reluctant to still use inquisitive applications like Google ones. We thus included MicroG services³ as well as a coherent set of default apps, and simplified the initial setup of the system. We also offer the way to uninstall default apps, in order to avoid users being trapped in an ecosystem. These apps can be easily restored, without requiring a network connection.
- To provide a new and powerful way of blocking ads, malware servers, and data leaks of any kind. We are developing a firewall, tightly integrated into the system, that captures all DNS requests and network traffic, as well as a user interface (the iodé app) to control the firewall and filter communications.

¹*Lineage Operating System*. URL: <https://github.com/LineageOS>.

²*Android Open Source Project*. URL: <https://source.android.com/>.

³*MicroG: A free-as-in-freedom re-implementation of Google's proprietary Android user space apps and libraries*. URL: <https://github.com/microg>.

Contents

1	AOSP/LineageOS changes to prevent data leaks to Google	4
1.1	Dialer proximity location	4
1.2	Domain Name System (DNS)	4
1.3	Connectivity check (Captive portal)	4
1.4	Assisted Global Positioning System (A-GPS)	4
1.5	Android System Webview	4
2	MicroG services and default apps	5
2.1	MicroG services	5
2.2	iodé	5
2.3	iodé News & FAQ	5
2.4	Aurora Store	6
2.5	F-Droid	6
2.6	iodé Browser	6
2.7	Pretty Easy Privacy (pEp)	7
2.8	Magic Earth Navigation & Maps	7
2.9	Geometric Weather	7
2.10	Carnet	7
2.11	OpenBoard	8
2.12	Open Camera	8
2.13	QKSMS	8
3	iodéOS built-in firewall	9
3.1	Hosts and lists classification	10
3.1.1	Default blocking lists	10
3.1.2	Customized lists	11
3.2	Statistics and audit	13
3.3	Advantages compared to other solutions	18

1 AOSP/LineageOS changes to prevent data leaks to Google

In standard Android Open Source Project (AOSP) as well as in LineageOS, dependencies to Google are found.⁴ We thus replaced the following settings to prevent data leaks.

1.1 Dialer proximity location

In default Android, Google gives approximate locations for incoming / outgoing phone calls. We have replaced Google's default location by OpenStreetMap.⁵

1.2 Domain Name System (DNS)

LineageOS uses AOSP default DNS servers, which are Google's DNS servers 8.8.8.8 and 8.8.8.4. We have replaced Google's DNS by Quad9's 'unblocked' server 9.9.9.10.⁶

1.3 Connectivity check (Captive portal)

In Android, a connectivity check is done to check that Internet can be reached on available networks. The Captive Portal default detection requests a Google domain (connectivitycheck.gstatic.com). We have replaced it by a portal from a German website providing IT security services.⁷

1.4 Assisted Global Positioning System (A-GPS)

LineageOS uses location reporting with Google's secure user plane location (SUPL) server (supl.google.com) for A-GPS. This helps in speeding up device positioning when using A-GPS, but each request to the server includes the device's International Mobile Equipment Identity (IMEI), International mobile subscriber identity (IMSI) along with the phone number.

We use a patch⁸ to avoid leaking personal data to SUPL server.

1.5 Android System Webview

Webview is a system application which offers basic browser capabilities and is called by many applications. It is based on the Chrome/Chromium rendering engine, and is not fully degoogled. However, unlike the previous items, we preferred not to replace it by a degoogled alternative. Indeed, this may break some of its functionalities, and thus the applications that use it. Instead, we rely on our firewall to block unwanted traffic.

⁴*How to deGoogle LineageOS in 2019.* Aug. 2019. URL: https://www.reddit.com/r/fossdroid/comments/clg2ca/how_to_degoogle_lineageos_in_2019_xpost/.

⁵*Open Street Map: The free wiki world map.* URL: <https://github.com/openstreetmap>.

⁶*Quad9: An open DNS recursive service for free security and high privacy.* URL: <https://www.quad9.net/>.

⁷*Kuketz IT.* URL: <http://captiveportal.kuketz.de>.

⁸*SUPL/IMSI patch.* URL: https://review.lineageos.org/c/LineageOS/android_frameworks_base/+249219/1.

2 MicroG services and default apps

2.1 MicroG services



MicroG⁹ is an open source replacement for Google Play Services, allowing applications to use services such as push notifications and geolocation.

Particularly, an initialization of MicroG has been made with:¹⁰

- Firebase Cloud Messaging (GCM) notifications allowed by default.
- Two location providers pre-selected: DéjàVu (works on self-learning and doesn't use the network) and Mozilla Network Location Provider (NLP).
- Nominatim geocoder backend enabled.
- Mapbox selected as default map tiles provider, as a replacement to Google Maps.

2.2 iodé



iodé is our built-in firewall's user interface application. From there the user can:

- analyze data (DNS) requests and network packets transmissions,
- control the firewall and block requests towards unwanted recipients,
- customize and combine blocking protections,
- measure the data confidentiality degree by each application.

The firewall will be explained in details in Section 3.

2.3 iodé News & FAQ



⁹*MicroG: A free-as-in-freedom re-implementation of Google's proprietary Android user space apps and libraries.*

¹⁰*GmsCore.* URL: <https://gitlab.com/iode/os/apps/GsfProxy>; *FakeStore.* URL: <https://gitlab.com/iode/os/apps/FakeStore>.

The News application notifies on iodé's updates and novelties. It also contains a Frequently Asked Questions section.

We are not using Google's firebase push notifications to fetch news. The device fetches iodé's gitlab¹¹ repository once per day to find any notifications.¹²

2.4 Aurora Store



Aurora Store¹³ is an alternative to Google's Play Store that lets the user connect to it anonymously, informs about in-app trackers, and has location and device spoofing options.

Paid apps from a Google account can also be retrieved from Aurora Store.

2.5 F-Droid



F-Droid¹⁴ is an alternative app store with exclusively open source apps.

We have added¹⁵ our repository 'Apps for iodéOS' with the following applications: iodé Browser, Open Camera, Jelly (LineageOS default browser), iodé's News, MicroG, F-Droid (to embed our own repository and avoid name conflicts of some apps) and Aurora store. The repository lets us quickly push updates and fixes if needed.

2.6 iodé Browser



iodé browser is a fork of Firefox¹⁶ with:¹⁷

- telemetry disabled,
- many trackers removed from code even if the disabled telemetry should avoid them on acting,

¹¹*iodéOS repository.* URL: <https://www.gitlab.com/iode>.

¹²*Flutter local notifications: A cross platform plugin for displaying local notifications.* URL: https://pub.dev/packages/flutter_local_notifications.

¹³*Aurora Store.* URL: <https://gitlab.com/AuroraOSS/AuroraStore>.

¹⁴*F-Droid.* URL: <https://f-droid.org>.

¹⁵*F-Droid, iodé fork.* URL: <https://gitlab.com/iode/os/apps/fdroid>.

¹⁶*Firefox.* URL: <https://github.com/mozilla-mobile/fenix>.

¹⁷*Iodé Browser, iodé fork.* URL: [Sourcecode:https://gitlab.com/iode/os/apps/IodeBrowser](https://gitlab.com/iode/os/apps/IodeBrowser); *Iodé Browser components.* URL: [Sourcecode:https://gitlab.com/iode/os/apps/iode-browser-components](https://gitlab.com/iode/os/apps/iode-browser-components).

- alternative search engines: Qwant (default), Brave, Ecosia, Metager, Qwant light, Startpage and several Searx instances.

2.7 Pretty Easy Privacy (pEp)



pEp¹⁸ is the default email client and simplifies encryption on mobile devices for everyone by automatically and seamlessly integrating end-to-end encryption.

2.8 Magic Earth Navigation & Maps



Magic Earth¹⁹ uses OpenStreetMap maps and an efficient search algorithm to provide optimal routes using real-time traffic.

2.9 Geometric Weather



Geometric Weather²⁰ is an open source Android weather app, giving real-time temperatures, daily and hourly forecasts and with the choice of different weather providers.

2.10 Carnet



Carnet²¹ is an open source powerful note-taking app.

¹⁸*Pretty Easy Privacy*. URL: <https://gitea.pep.foundation/pEp.foundation>.

¹⁹*Magic Earth*. URL: <https://www.magicearth.com/>.

²⁰*Geometric Weather*. URL: <https://github.com/WangDaYeeyeeeee/GeometricWeather>.

²¹*Carnet*. URL: <https://github.com/CarnetApp/CarnetFdroid>.

2.11 OpenBoard



OpenBoard²² is an open source keyboard based on AOSP keyboard that does not depend on Google binaries. The keyboard supports spell correction, themes and emojis.

2.12 Open Camera



Open Camera²³ is a feature rich camera application including: auto-stabilise option, multitouch zoom, flash/torch, choice of focus modes, face detection, front/back camera support, change recording resolution, video/audio recording, timer, burst mode, silenceable shutter, configurable gui, geotagging, external microphone support. We made a few modifications²⁴ such as API v2 by default and more tools in the top bar.

2.13 QKSMS



QKSMS²⁵ is a clean open source SMS app with many features like Group Messages, Backup and Restore, MMS, Search, Dual SIM support, Delayed Message Sending and Blacklist to block numbers.

²² *OpenBoard*. URL: <https://github.com/dslul/openboard/>.

²³ *Open Camera*. URL: <https://sourceforge.net/projects/opencamera/>.

²⁴ *Open Camera, iodé fork*. URL: <https://gitlab.com/iode/os/apps/OpenCamera>.

²⁵ *QKSMS*. URL: <https://github.com/moezbhatti/qksms>.

3 iodéOS built-in firewall

iodéOS built-in firewall/adblocker is tightly integrated into the system and relies on a hacking principle called “man-in-the-middle attack” (MITM), with the end goal of intercepting communications between 2 endpoints. Here, the blocker plays the MITM role and intercepts by default all DNS requests and network traffic while the device is turned ON.

The firewall automatically blocks by default every DNS requests towards ”unwanted” hosts and presents many features to the user that will be explained in the following sections such as the possibility to:

- analyze authorized and blocked DNS requests from each app and to different hosts,
- map the quantity of network traffic between apps and hosts,
- view a world map of the traffic linked to each country,
- enable and combine several levels of blocking lists per app,
- customize lists per app,
- audit the data confidentiality degree per app,
- clear statistics and turn OFF the firewall.

We are actively developing the firewall, and new functionalities will be regularly added.

3.1 Hosts and lists classification

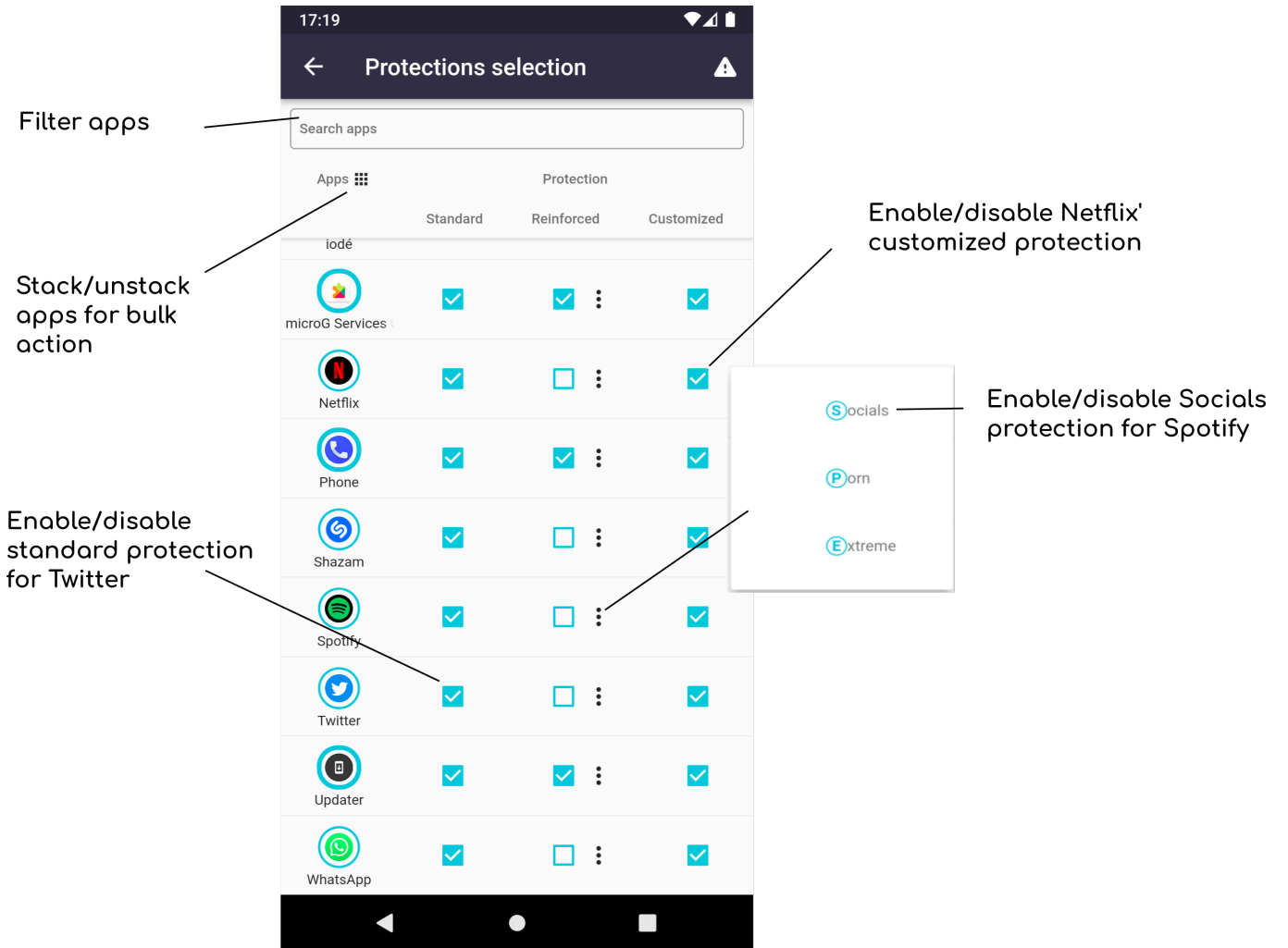


Figure 1: Protection selection settings

3.1.1 Default blocking lists

To classify "unwanted hosts" to block by default, we rely on an open source collaborative database²⁶ that we update at each Over-The-Air (OTA) iodéOS update. The database defines these hosts as "advertisements, malwares, spams, spyware, statistics and trackers",²⁷ We named it "standard protection", including 400k recipients.

We also defined a "reinforced protection" including subcategories of lists:

- Socials²⁸ containing social network hosts (~4k),

²⁶ Energized Basic Pack. URL: <https://block.energized.pro/basic/formats/hosts.txt>.

²⁷ Energized Protection block repository. URL: <https://github.com/EnergizedProtection/block>.

²⁸ Energized Ultimate Pack. URL: <https://block.energized.pro/extensions/social/formats/domains.txt>.

- Porn²⁹ containing sexual content hosts (~300k),
- Extreme³⁰³¹³² containing a wider list of "unwanted" hosts (~600k).



If one app malfunctions, it may be due to an enabled protection being too restrictive. The user might want to disable each of the app's protections one by one until it works, or directly disable them all.

3.1.2 Customized lists

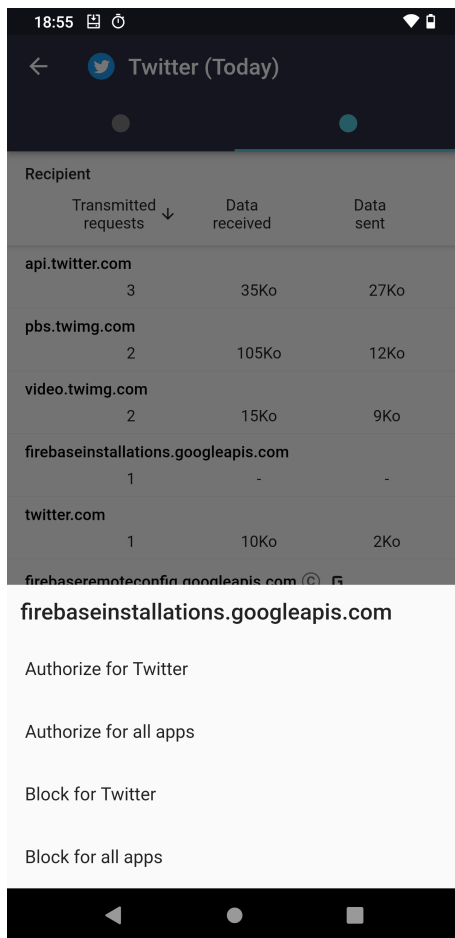


Figure 2: Customization of a Google host (firebaseinstallations.googleapis.com)

²⁹ *Energized Ultimate Pack*. URL: <https://block.energized.pro/porn/formats/hosts.txt>.

³⁰ *Energized Ultimate Pack*. URL: <https://block.energized.pro/ultimate/formats/hosts.txt>.

³¹ *Energized Ultimate Pack*. URL: <https://block.energized.pro/extensions/regional/formats/domains.txt>.

³² *Energized Ultimate Pack*. URL: <https://block.energized.pro/extensions/xtreme/formats/domains.txt>.

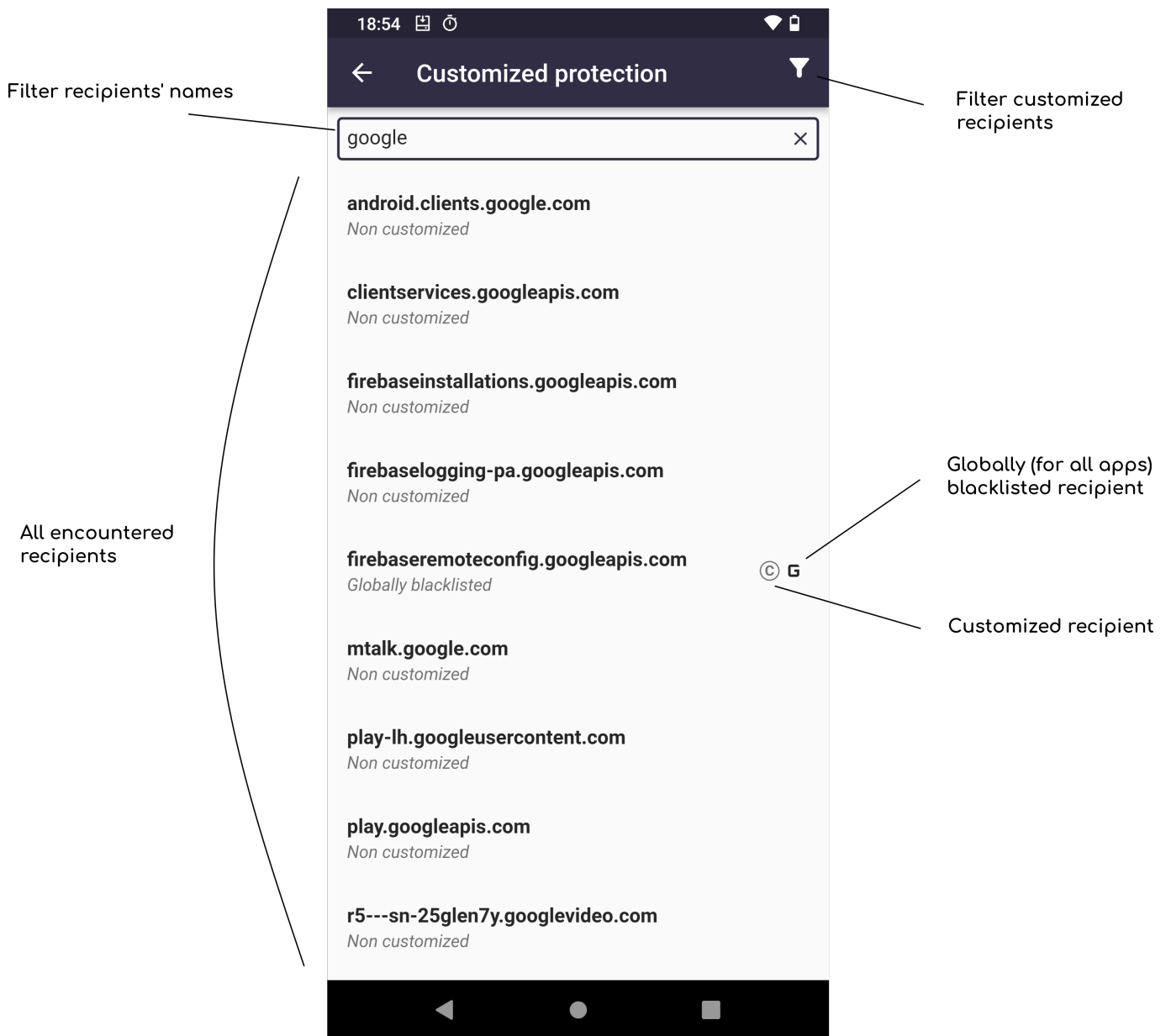


Figure 3: Management of (customized) hosts

In addition to iodé's provided protections, the user can customize his own 'Customized protection'. This means:

- add/remove any given host to an app or all apps' customized blacklist and whitelist (see Figure 2),
- view the whole list of hosts and manage customized hosts (see Figure 3),
- enable/disable the customized protection for any app, or all apps (see Figure 1).



A grey 'G' symbol next to a host name means the host is globally (all apps) blacklisted
A blue 'G' symbol next to a host name means the host is globally (all apps) whitelisted
Individual blocking (per app) has priority over global blocking (all apps).

3.2 Statistics and audit

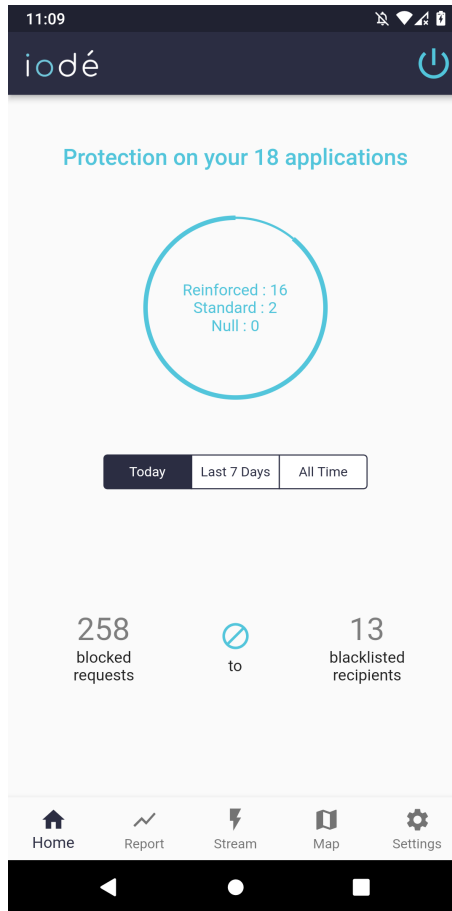


Figure 4: Home page

The home page (Figure 4) lets the user see what protection is being enabled for each app, and how many DNS requests and hosts were globally blocked on the phone for a given timeframe (Today, Last 7 Days, All Time). In the above example, out of 18 apps, 16 apps are protected by the reinforced protection, while 2 are with the standard one.

258 requests and 13 recipients were blocked the same day.

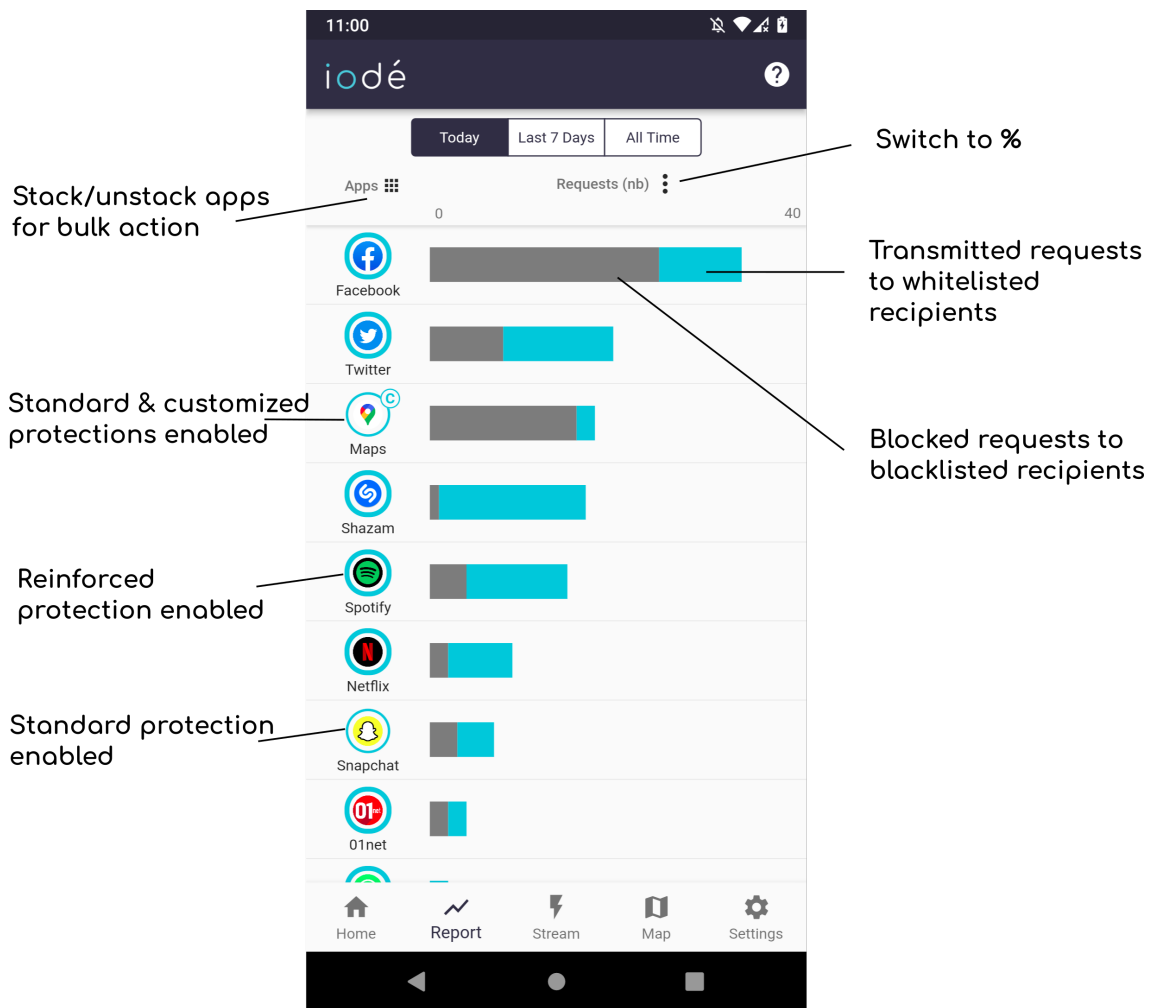


Figure 5: Report page with stats per app

The report tab (Figure 5) displays in a bar graph how many DNS requests were blocked and authorized (in number or percentage) for each app for a given timeframe (Today, Last 7 days, all time). The blocked requests/authorized requests ratio helps measuring the data confidentiality respect by each app.

11:19

Family Island (Last 7 Days)

Domain	Blocked requests ↓	Data received	Data sent
graph.facebook.com	1809	-	-
fi-analytics.mgsn.it	211	-	-
init.supersonicads.com	109	-	-
app.adjust.com	75	-	-
outcome-ssp.supersonicads.com	24	-	-
inapps.appsflyer.com	17	-	-
events3alt.adcolony.com	13	-	-
launches.appsflyer.com	7	-	-
cdn-creatives-akamaistls-prd.unityads.unity3d.com	5	-	-
googleads.g.doubleclick.net	4	-	-

Figure 6: Family Island's blocked DNS requests










Recipient	Transmitted requests ↓	Data received	Data sent
android.prod.cloud.netflix.com	28	-	429Ko
android-appboot.netflix.com	3	-	15Ko 
assets.nflxext.com	1	-	19Ko 
eu-aa.online-metrix.net	1	-	- 
eu-aa.online-metrix.net.	1	-	1Ko 
h.online-metrix.net	1	-	4Ko 
lg9m47phnpqnkdmynve45zfqxzoyb2w4h...	1	-	1Ko 
secured.netflix.com	1	-	31Ko 
www.googleapis.com	1	-	6Ko 
www.netflix.com	1	-	4Ko 

Figure 7: Netflix's authorized DNS requests and network traffic

The user can view in details per app and per host how many requests were blocked/authorized (Figures 6 and 7); as well as the traffic and country associated (if applicable).

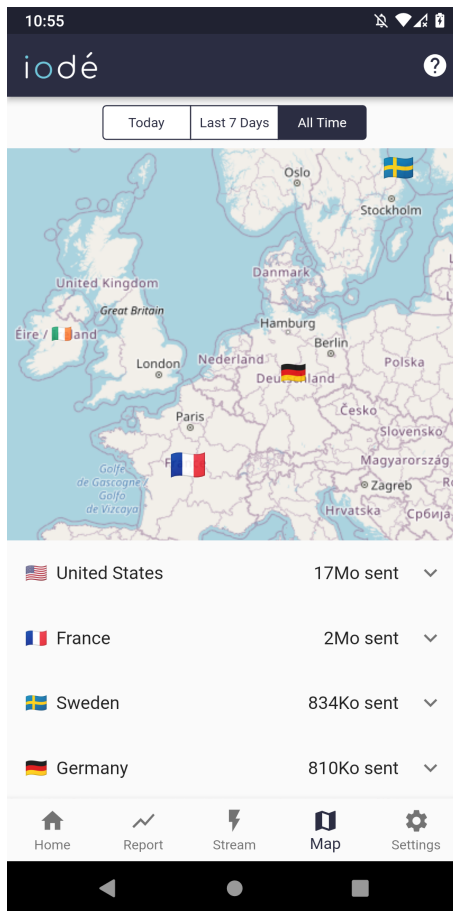


Figure 8: World map data traffic

A map section (Figure 8) displays data sent from the system per country per host and per timeframe. We use Maxmind's Geolite database³³ to locate recipients.

³³ *GeoLite2 Free Geolocation Data*. URL: <https://dev.maxmind.com/geoip/geolite2-free-geolocation-data>.

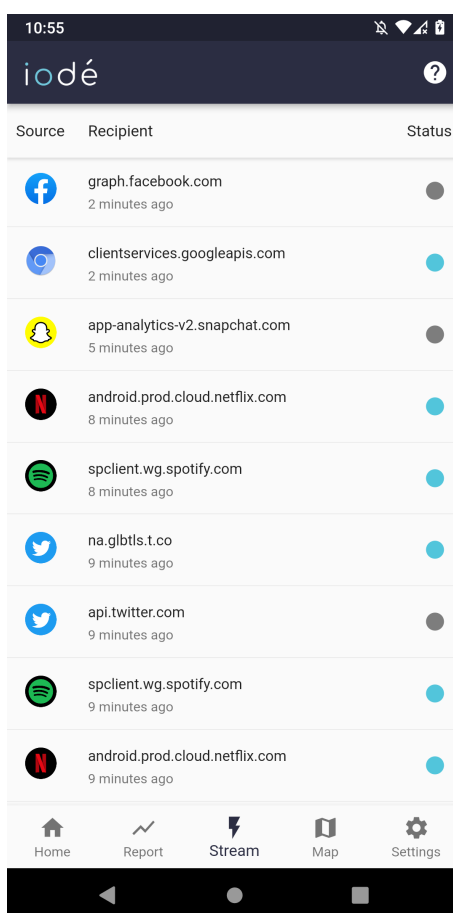


Figure 9: DNS requests Stream

The stream tab (Figure 9) displays the previous 30 minutes blocked and transmitted requests from each app to each recipient.

This tab also lets the user add/remove any given host to an app or all apps' customized blacklist and whitelist such as from the report's tab in figure 2.

3.3 Advantages compared to other solutions

Compared to some other well-known firewalls, iodéOS's firewall has the advantages of:

- Avoiding to lock the VPN for that use. You can even use another adblocker/firewall that uses VPN technology alongside our blocker.
- Being independent of the kind of DNS server used by the system or set by an independent app: classical DNS on UDP port 53 or any other one, DNS over TLS (DoT), DNS over HTTPS (DoH), ..., as we capture the DNS requests before they are transmitted to the system function that emits the DNS request. What we do not support, is DoH when it is natively built into applications, i.e. when an app communicates directly with a DoH server, without asking name resolution to the system. It would require to decrypt HTTPS packets between such an app and the DoH server, which may create a big security hole.

- Letting the user have a fine-grained audit on internet communications, and a large control over the firewall with freedom to classify each encountered hosts and customize apps filtering

References

- Android Open Source Project*. URL: <https://source.android.com/>.
- Aurora Store*. URL: <https://gitlab.com/AuroraOSS/AuroraStore>.
- Carnet*. URL: <https://github.com/CarnetApp/CarnetFdroid>.
- Energized Basic Pack*. URL: <https://block.energized.pro/basic/formats/hosts.txt>.
- Energized Protection block repository*. URL: <https://github.com/EnergizedProtection/block>.
- Energized Ultimate Pack*. URL: <https://block.energized.pro/extensions/social/formats/domains.txt>.
- Energized Ultimate Pack*. URL: <https://block.energized.pro/porn/formats/hosts.txt>.
- Energized Ultimate Pack*. URL: <https://block.energized.pro/ultimate/formats/hosts.txt>.
- Energized Ultimate Pack*. URL: <https://block.energized.pro/extensions/regional/formats/domains.txt>.
- Energized Ultimate Pack*. URL: <https://block.energized.pro/extensions/xtreme/formats/domains.txt>.
- F-Droid*. URL: <https://f-droid.org>.
- F-Droid, iodé fork*. URL: <https://gitlab.com/iode/os/apps/fdroid>.
- FakeStore*. URL: <https://gitlab.com/iode/os/apps/FakeStore>.
- Firefox*. URL: <https://github.com/mozilla-mobile/fenix>.
- Flutter local notifications: A cross platform plugin for displaying local notifications*. URL: https://pub.dev/packages/flutter_local_notifications.
- GeoLite2 Free Geolocation Data*. URL: <https://dev.maxmind.com/geoip/geolite2-free-geolocation-data>.
- Geometric Weather*. URL: <https://github.com/WangDaYeeeeee/GeometricWeather>.
- GmsCore*. URL: <https://gitlab.com/iode/os/apps/GsfProxy>.
- How to deGoogle LineageOS in 2019*. Aug. 2019. URL: https://www.reddit.com/r/fossdroid/comments/clg2ca/how_to_degogoogle_lineageos_in_2019_xpost/.
- Iodé Browser components*. URL: Sourcecode:<https://gitlab.com/iode/os/apps/iode-browser-components>.
- Iodé Browser, iodé fork*. URL: Sourcecode:<https://gitlab.com/iode/os/apps/IodeBrowser>.
- iodéOS repository*. URL: <https://www.gitlab.com/iode>.
- Kuketz IT*. URL: <http://captiveportal.kuketz.de>.
- Lineage Operating System*. URL: <https://github.com/LineageOS>.
- Magic Earth*. URL: <https://www.magicearth.com/>.
- MicroG: A free-as-in-freedom re-implementation of Google's proprietary Android user space apps and libraries*. URL: <https://github.com/microg>.
- Open Camera*. URL: <https://sourceforge.net/projects/opencamera/>.
- Open Camera, iodé fork*. URL: <https://gitlab.com/iode/os/apps/OpenCamera>.
- Open Street Map: The free wiki world map*. URL: <https://github.com/openstreetmap>.
- OpenBoard*. URL: <https://github.com/dslul/openboard/>.
- Pretty Easy Privacy*. URL: <https://gitea.pep.foundation/pEp.foundation>.
- QKSMS*. URL: <https://github.com/moezbhatti/qksms>.
- Quad9: An open DNS recursive service for free security and high privacy*. URL: <https://www.quad9.net/>.
- SUPL/IMSI patch*. URL: [https://review.lineageos.org/c/LineageOS/android_frameworks_base/+/
249219/1](https://review.lineageos.org/c/LineageOS/android_frameworks_base/+/).