PROTELION
GOVERNMENT SOLUTIONS

Protelion ArmoredMobile Glossary

2:45
2:31
Fri, Apr 18

Contents

Protelion ArmoredMobile Key Features

Protelion ArmoredMobile is a holistic solution that enables highly secure mobile device communication, featuring the Protelion ArmoredMobile with meticulously crafted security measures. Off-the-shelf Android mobile phones were hardened by implementing Protelion's developed Android-based ArmoredOS, a highly secure, fully customized mobile phone OS.

The ArmoredMobile Smartphone supports an always-on VPN with customized Protelion and system apps for improved security and functionality.

Protelion ArmoredMobile solution includes:

- ArmoredOS, a mobile OS with enhanced security system
- A corporate app store
- A centralized mobile device management system
- Protelion AR VPN and Protelion AR Messenger

Protelion ArmoredMobile Key Features are:

- Always-on VPN by design
- Protection of messages, voice calls, and video calls with Protelion AR Messenger
- Zero-day exploits protection using powerful hardened mechanisms
- Preventing surveillance and attacks through unused adapters (WiFi, Bluetooth, NFC)
- Preventing phone call interception and attacks via GSM
- Installing applications from a particular server of a secure application store on the client's corporate network
- More secure method of creating processes than in a traditional AOSP
- Control and isolation of low-level untrusted components
- Up-to-time secure OTA updates from a special server on the client's corporate network
- Absence of Google Mobile Services and Accessibility features in the operating system
- Allows the client to control all device network traffic through the VPN tunnel
- Ability to integrate with IDS/IPS and Security Operation Centers (SOC)
- Real-time Kernel-mode antivirus checking in all files on the system
- Built-in DNS block filter for ads and malware hosts
- Verified boot using the Protelion key (root-of-trust)
- Protection against firmware flashing and modification

- PIN-code bypass protection
- Protection against mobile forensics tools
- Anti-snatch feature based on ML algorithms
- The ability to use the own MDM system for centralized management devices

More unique features of the Protelion ArmoredMobile are:

- Protects device at the kernel level
- Isolates device traffic completely (VPN)
- Allows installing only trusted apps with platform signature
- Protects corporate data using Protelion Secure Communication
- Provides centralized internet access management
- Ensures secure access to internal corporate resources
- Enables centralized device management capability

Security measures implemented in Protelion ArmoredMobile:

- **To counter cyber threats:**

  - Data is transmitted in encrypted form. Non-VPN connections are blocked for all OS components. Protection is due to a kernel-level firewall and Protelion AR VPN
  - The pre-installed Protelion AR Messenger application is used to protect corporate correspondence and calls
  - The list of Protelion AR Messenger users is maintained by the customer's network administrator
  - The 2G mode is turned off by default, and GSM calls can be prohibited to protect against IMSI-catchers and GSM call interception

- **A random MAC address is generated for each Wi-Fi connection, and unused adapters (NFC, Wi-Fi, and Bluetooth) are automatically turned off to protect against tracking and attacks through adapters. To counter app threats:**

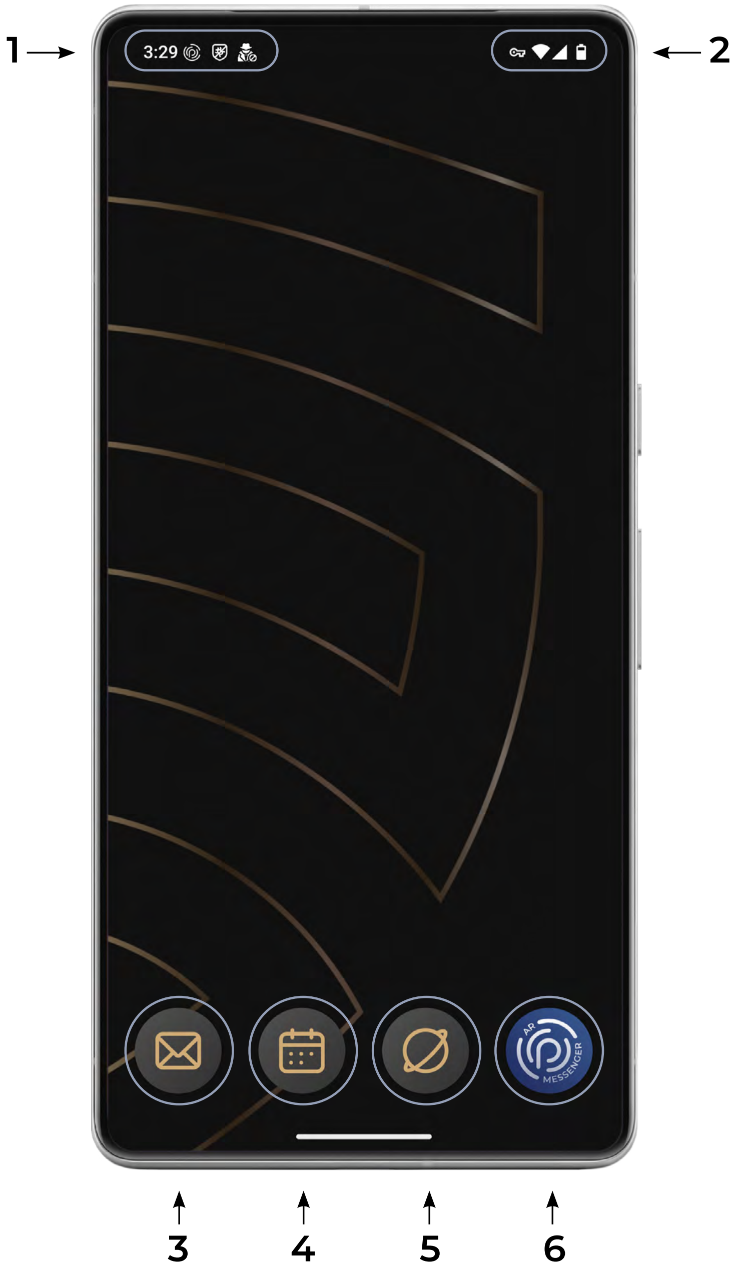
  - Data is transmitted in encrypted form. Non-VPN connections are blocked for all OS components. Protection is due to a kernel-level firewall and Protelion AR VPN
  - The pre-installed Protelion AR Messenger application is used to protect corporate correspondence and calls
  - The list of Protelion AR Messenger users is maintained by the customer's network administrator
  - The 2G mode is turned off by default, and GSM calls can be prohibited to protect against IMSI-catchers and GSM call interception

- **To counter OS threats:**
  - The following secure system and components protect the device against the zero-day vulnerability exploit:
    - Memory allocator (hardened malloc)
    - Hardened kernel and Libc library
    - Browser and WebView component
    - Office and PDF Viewer applications for secure document viewing
    - Camera application for secure QR code scanning
  - ArmoredOS features built-in system for isolating the GPS driver and the microphone driver
  - The OS is updated through timely OTA (over-the-air) updates within the corporate network, due to hosting the OS update server as a virtual machine image within the corporate network
  - The following have been removed from ArmoredOS:
    - Support for screen reader applications in “Accessibility”: prevents apps from tracking users’ activities
    - Google Mobile Services (GMS): prevents tracking, managing, and blocking through these services
  - “Paranoia” simultaneously turns off the cellular modem, Wi-Fi, Bluetooth adapter, camera, microphone, sensors, and location detection
  - You can completely turn off location tracking on the device during setup. In this case, you can use the device location tracking feature only after resetting it to factory defaults
  - Connecting a USB device is possible only when the screen is unlocked

- **To counter device threats:**
  - The bootloader is locked, and the Root of Trust technology is used to protect against tampering and modifications to the device OS. The loaded OS image integrity is verified through the Protelion ArmoredMobile keys. The device is protected against downgrading to older OS versions
  - ArmoredOS has no Developer Mode and bootloader unlock features
  - To protect against unauthorized access, you can turn on:
    - Key input layout scrambling on PIN entry. The PIN entry keys change positions each time to protect against shoulder surfing.
      The feature is on by default
    - Automatic deletion of user data in ArmoredMobile after multiple failed attempts to enter a PIN. By default, 11 attempts are allowed
    - Data deletion in ArmoredMobile when you enter a special PIN.
      You configure the feature on device setup. It is off by default
  - To protect against unauthorized access to information on the device upon theft, Protelion ArmoredMobile is locked as soon as an attacker takes it

Protelion ArmoredMobile Interface

The picture below provides a brief explanation of Protelion ArmoredMobile interface is presented.



1. The icons presented on the figure above are as follows (from the left to the right accordingly):

- **Clock** - current time
- **Protelion logo** - Protelion AR VPN is enabled
- **Shield** - System is under protection

- **Man with a hat** - the Anti-Snatch service is activated. If an intruder grabs the device during a call, it will be locked immediately. However, it remains unlocked when the phone is dropped or other unintentional actions, as the machine-learning algorithm relies on data from the snatching detection sensor.

2. The icons presented on the figure above are as follows (from the left to the right accordingly):

- **Key** - the Protelion AR VPN application is running. Your device's network traffic is protected. You can safely work with email, apps and websites
- **Wi-Fi** - a device is connected to a Wi-Fi network
- **Signal** - a SIM card is ON and Mobile data is activated
- **Battery** - a charge level

3. Corporate Email Application

4. Calendar

5. Web Browser

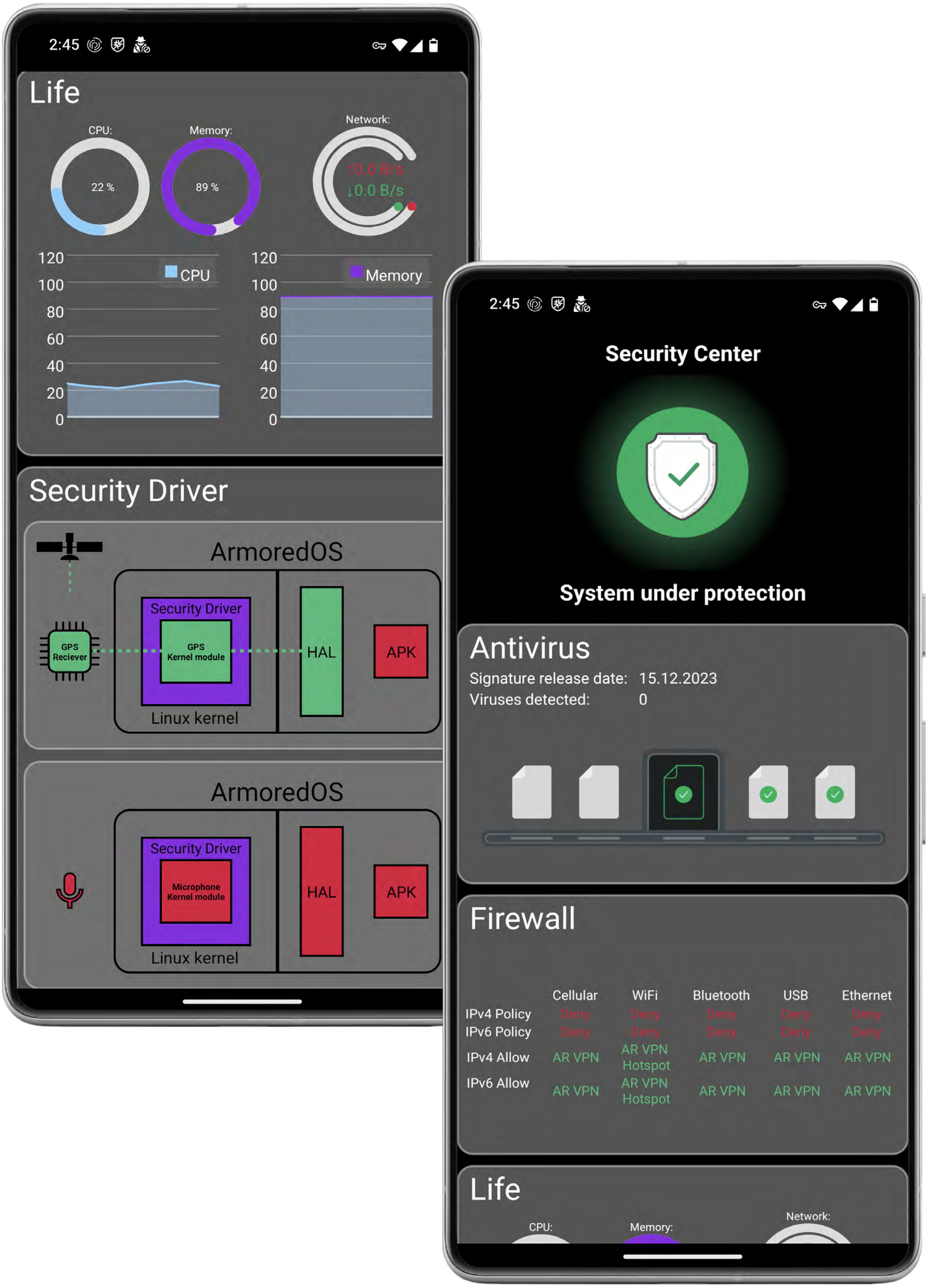
6. Protelion AR Messenger

> “ The ArmoredMobile Smartphone supports an always-on VPN with customized Protelion and system apps for improved security and functionality. ”

Embedded application for visualizing and monitoring device protection mechanisms are presented in the Security Center, see figure below (page 9).

- Kernel-level antivirus
  - real-time hash and YARA signature scanning of all system files
- System Firewall
  - network access restriction rules for OS components and applications
- System life status monitoring
  - CPU, memory and network utilization monitoring from OS kernel level
- Monitoring of isolation untrusted components
  - microphone, camera and GPS isolation core modules visualization

- Adapters activity
  - cellular modem, WiFi, Bluetooth, NFC and USB activity monitoring
- Applications permission control
  - control app permission for camera, microphone, GPS and sensors



Signature release date: 15.12.2023
Viruses detected: 0

	Cellular	WiFi	Bluetooth	USB	Ethernet
IPv4 Policy	Deny	Deny	Deny	Deny	Deny
IPv6 Policy	Deny	Deny	Deny	Deny	Deny
IPv4 Allow	AR VPN	AR VPN Hotspot	AR VPN	AR VPN	AR VPN
IPv6 Allow	AR VPN	AR VPN Hotspot	AR VPN	AR VPN	AR VPN

Protelion ArmoredMobile Glossary

A

Aegis
An Authenticator to manage your 2-step verification tokens for your online services.

aFreeRDP
Remote Desktop Protocol client.

AOSP
Android Open Source Project is an operating system project for Android with fully open source code.

Always-on VPN
Deny any connections bypassing VPN.

Antivirus
Built-in kernel-level antivirus that runs signature-based scanning of all system files in real-time by hash values and YARA rules.

ArmoredOS
A mobile OS with enhanced security system.

B

Built-in DNS block filter
To block ads and malware webpages.

C

CalDAV
An internet standard for managing calendars, task lists, and providing shared access to them.

Corporate App Store
Corporate App Store is an application server (virtual machine image) with two components:

- ArmoredMobile Update Server, which is responsible for ArmoredOS OTA updates
- ArmoredMobile Apps Server, which is responsible for installing and updating apps over the air on Protelion ArmoredMobile devices

D

DAVx

Is a CalDAV/CardDAV management and synchronization app for Android, which natively integrates with Android calendar/contact apps.

E

EDS Lite

“Encrypted Data Store” is a virtual disk encryption software for Android, which allows you to store your files in an encrypted container.

G

GSM

Global System for Mobile communication is a digital mobile network that is widely used by mobile phone users in Europe and other parts of the world.

I

IDS

An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations.

IMEI

International Mobile Equipment Identity is a unique 15-digit serial number for identifying a device; every mobile phone in the world has one.

IMSI

International Mobile Subscriber Identity (IMSI) number is used to identify a specific user. IMSI is usually stored on a Subscriber Identity Module (SIM), a smart card issued by the user’s provider, which also contains a shared secret, meaning a key exchange (KE) which can then be used to secure an interface between mobile device and a smart card (SIM, UICC).

IMSI-Catcher

An IMSI-Catcher is a device used to:

- Masquerade as a base station
- Collect the IMSIs of users in a target area by indicating to the holder of an unknown TMSI that the TMSI is invalid, thus triggering the sending of the IMSI by the mobile phone user

- Track/or locate a specific IMSI using signal strength and signal propagation delay to place the attacker as a man-in-the-middle. User establishes a connection with the fake base station. IMSI-Catcher establishes another connection to a real base station, to forward communication

IPS
Intrusion Prevention System (IPS) is a network security device or software application that monitors network traffic and takes automated actions
to prevent potential threats and unauthorized access.

J

Jitsi Meet
Video conferences application.

K

KeePassDX
Is a password manager for Android, which helps you manage your passwords
in a secure way.

M

MDM
Mobile Device Management system that enables:

- Retrieving the device details:
  - IMEI, serial number, phone number, battery charge
  - Network connections data
- Mapping the device location and store its movement history
- Managing devices remotely:
  - Instant delivery of MDM system notifications
  - Device wiping, rebooting, and screen locking
  - PIN changing functionality
- Sending configurations (policies) to device groups to:
  - Configure security policies
  - Install applications
  - Block the camera, microphone, location, and adapters
  - Forbid screen capturing

N

Nextcloud
Synchronization client for your data, calendars, contacts and so on.

NewPipe

Video Streaming client.

NFC

“Near-field communication” is a set of communication protocols that enables communication between two electronic devices over a short distance.

O

OpenKeychain

OpenKeychain is based on the well-established OpenPGP standard making encryption compatible across devices and systems. It’s based on digital keys, stores and manages your keys, and those of the people you communicate with, on your smartphone. OpenKeychain helps you communicate more privately.

OTA

Over-the-air updates.

P

“Paranoia” Mode

Simultaneously turns off the cellular modem (activates Airplane Mode), as well as Wi-Fi modem, Bluetooth adapter, camera, microphone, sensors, and location detection.

PGP

“Pretty Good Privacy” is an encryption program that provides cryptographic privacy and authentication for data communication.

Prohibiting 2G calls

For protecting against IMSI-Catcher attack.

Protelion AR Messenger

An application to protect corporate correspondence and calls.

Protelion AR VPN

An application for accessing the hosts within the Protelion network and encrypting host connections.

R

Root of Trust technology

Is used to protect against tampering and modifications to the device OS.

S

Surveillance Protection

Surveillance Protection includes:

- Random MAC address for each Wi-Fi connection
- Always-on VPN. Deny any connections bypassing VPN
- Complete rejection of Google services
- Removal of all tracking software components, detection and blocking of all requests to external services
- Random MAC address for each Bluetooth connection
- Automatic disconnection of unused sensors and adapters. Disabling sensors (NFC, etc.) and Wi-Fi, Bluetooth adapters
- ''Paranoia mode'' - software button for disabling a camera, microphone, adapters and sensors at the system level, possibly with the use of NFC

V

VLC

Video and Music player.

Y

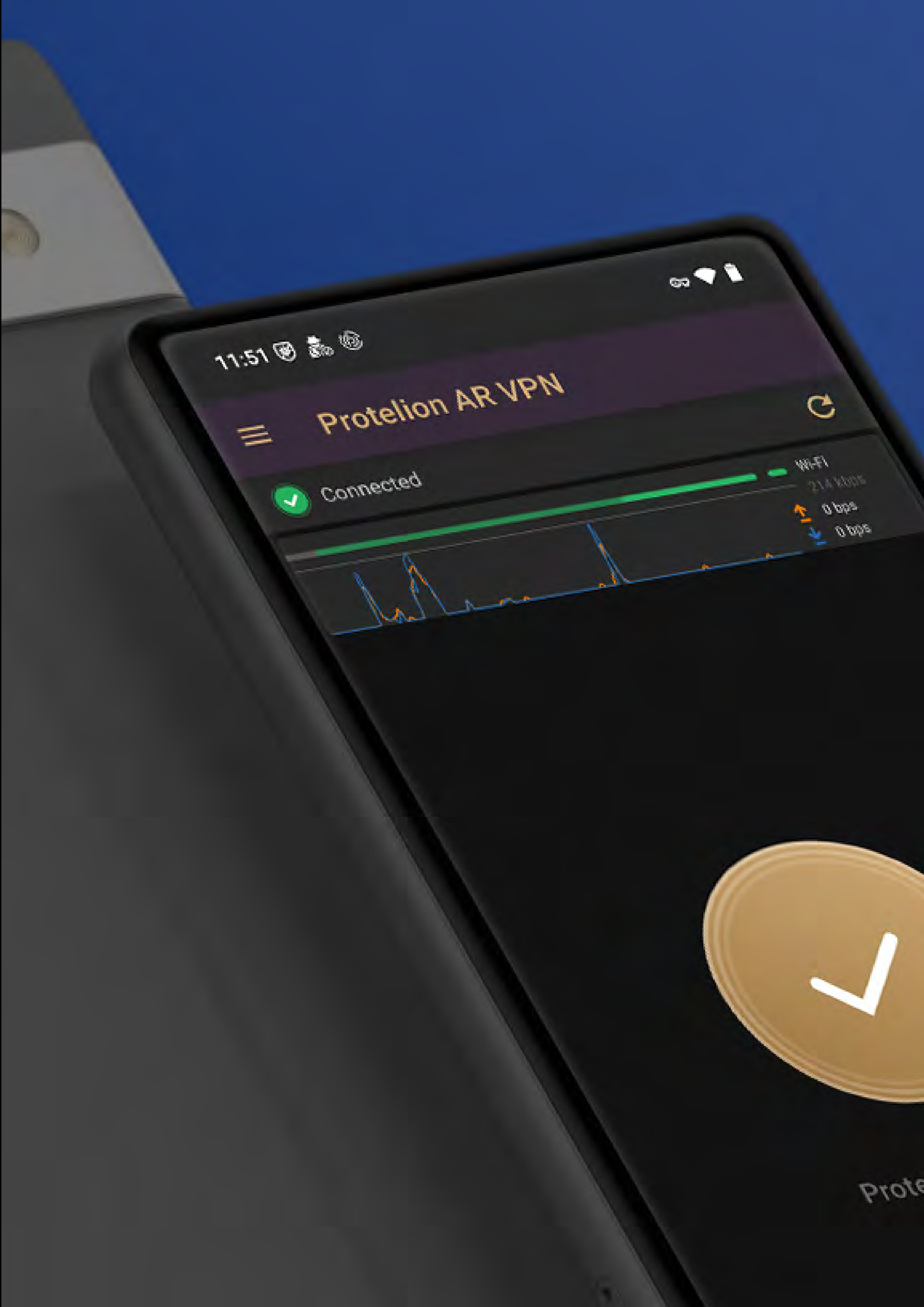
YARA Rules

"Yet Another Ridiculous Acronym" is a pattern-matching framework used to identify and classify malware and other IT security threats.

Z

Zero-day exploits

Is a vulnerability in software or hardware that is typically unknown to the vendor and for which no patch or other fix is available.


11:51
Protelion AR VPN
Connected
Wi-Fi
214 kbps
0 bps
0 bps
Prote

PROTELION
GOVERNMENT SOLUTIONS

Oberwallstr. 24
D-10117 Berlin,
Germany

+49 30 206 43 66-50

gov@protelion.com

gov.protelion.com