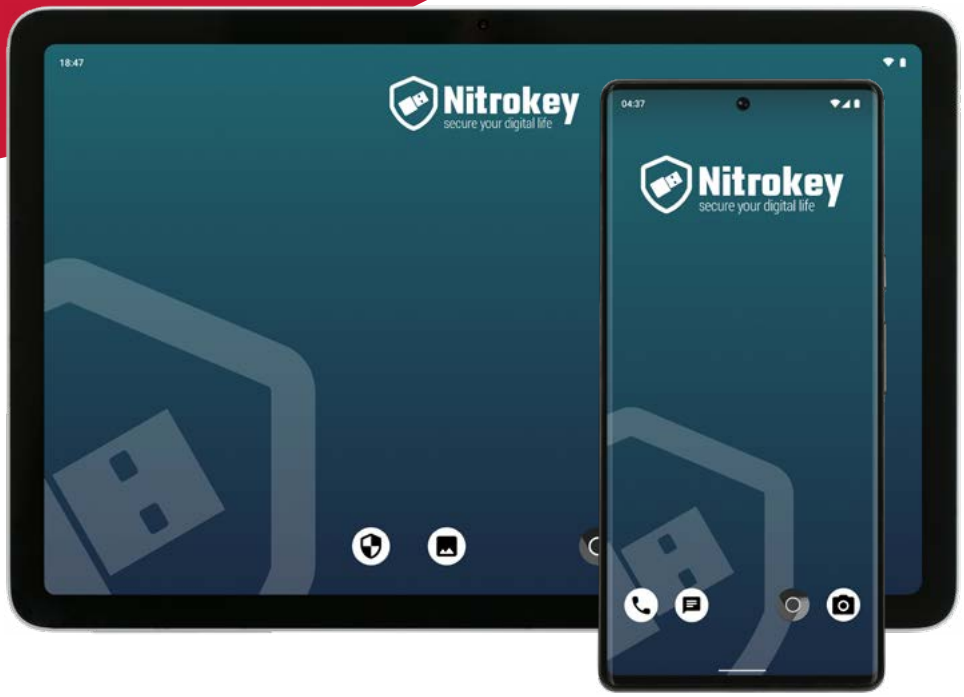
Nitrokey
secure your digital life



NitroPhone, NitroTablet

The Most Secure Android on the Planet

The NitroPhone and NitroTablet combine security, privacy and ease of use with modern hardware. Long-term software updates of 5 years guarantee sustainability and a low price per time. The NitroPhone and NitroTablet are based on the high-quality Pixel hardware and GrapheneOS, the most hardened Android for professionals.

- **Security: Hardened Android and hardware security for professional demands.**
- **Privacy: 100% open source under your control without Google and Apple.**
- **Optional: Removal of microphones, sensors, cameras and radio modules make eavesdropping of the environment physically impossible. Phone calls are made with optional headset.**

„NitroPhone is a much better product than we did with Blackphone.“

Phil Zimmermann, inventor of PGP

„If I were configuring a smartphone today, I‘d use Daniel Micay‘s GrapheneOS as the base operating system. I‘d desolder the microphones.“

Edward Snowden, NSA whistleblower

Physical Tamper Protection

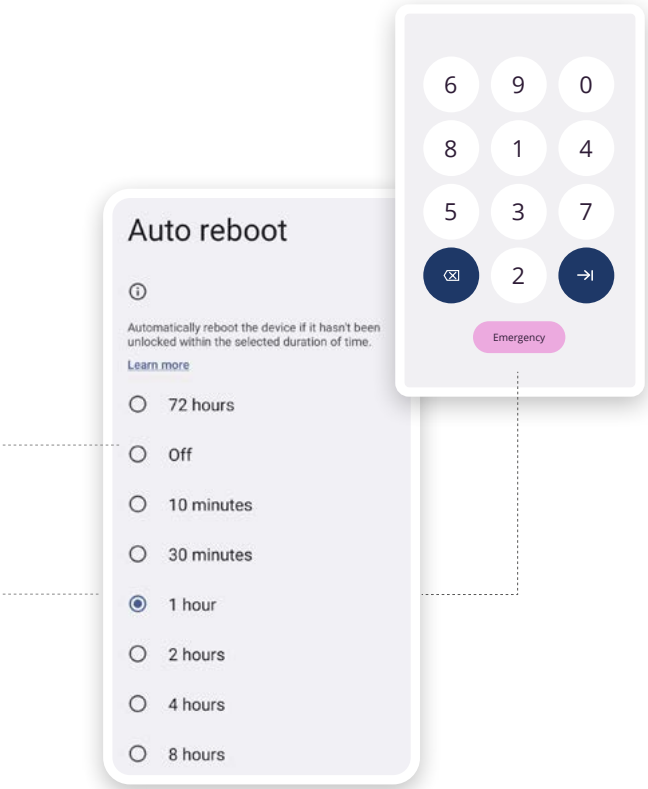
Strong encryption and Titan security chip protect your device and data against sophisticated physical attacks.

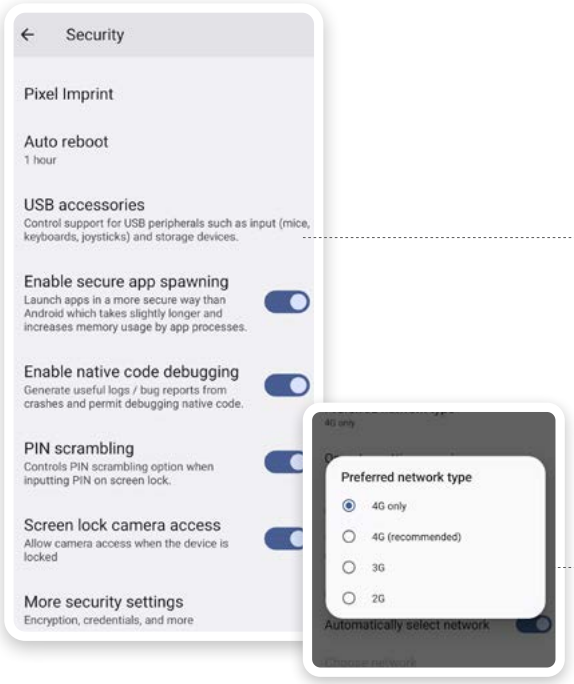
Verified boot ensures that your operating system has not been modified.

Automatic kill switch: Automatically shutdown after inactivity of configured time period.

PIN layout scrambling, together with privacy screen (not included), allow entering PIN in public without being watched. Alternatively: integrated fingerprint sensor.

The NitroPhone and NitroTablet are delivered in a **sealed box.**





Protection From Spyware and Zero-Day Exploits

Substantially hardened Android for high security demands (e.g. hardened stock apps, libc, malloc, compiler toolchain, kernel, filesystem access, WebView).

All apps are **sandboxed** to protect against exploitable and malicious apps.

Hardened browser, WebView and PDF viewer.

Protection against over-the-air exploits by isolating the baseband radio processor using IOMMU and optional LTE-only mode to significantly reduce cellular radio attack surface.

Optional: Without Microphones, Sensors, Cameras, Radio Modules

Optional: For very high security requirements, all microphones, cameras, acceleration and rotation sensors can be removed. This is because acceleration and rotation sensors could be misused as microphones. This physically prevents conversations in the environment from being eavesdropped. Phone calls can still be made with an external headset. With the NitroTablet, all wireless modules can be removed as well.

Privacy Protection: No Tracking, No Google

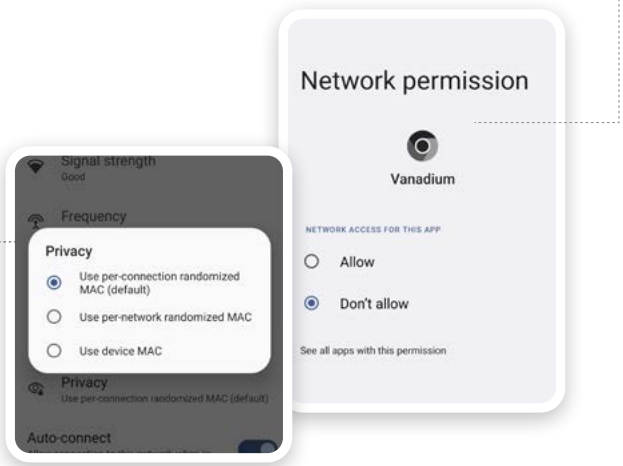
No cloud or Google Play Services integration by default, all under your control. If required, original Google Play Services can be installed as sandboxed apps without special privileges. This novel approach leads to much better compatibility than incomplete reimplementations like microG while providing higher security.

Tracking protection: Apps can't access device IMEI and serial numbers, SIM card serial numbers, subscriber ID, MAC address etc.

Per-connection MAC randomization **prevents tracking** by nearby WiFi scanners.

Firewall: Granular network and sensors permissions (e.g. GPS) toggle for each app.

Default Indicators for active camera, microphone, and location.



Secure Messenger

We recommend the end-to-end encrypted and **privacy-friendly messengers Signal and Nitro-Chat.** Alternatively, you can run Matrix on on your own server.

selection

MODERN HARDWARE

The NitroPhone is available in different versions between modern mid-range and high-end quality. It is also available as a large-format NitroTablet.

Inexpensive and Sustainable

Security updates over 5 years

For industrialized smartphones and tablets, a long lifespan is the most effective way to reduce resource consumption per user. As with hardly any other Android device, security updates are provided for the NitroPhone and NitroTablet for up to 5 years. Calculated over this lifetime, the phone costs only a few cents per day.

Quick repair

The NitroPhone and NitroTablet can be opened relatively easily for repair and defective components can be replaced.

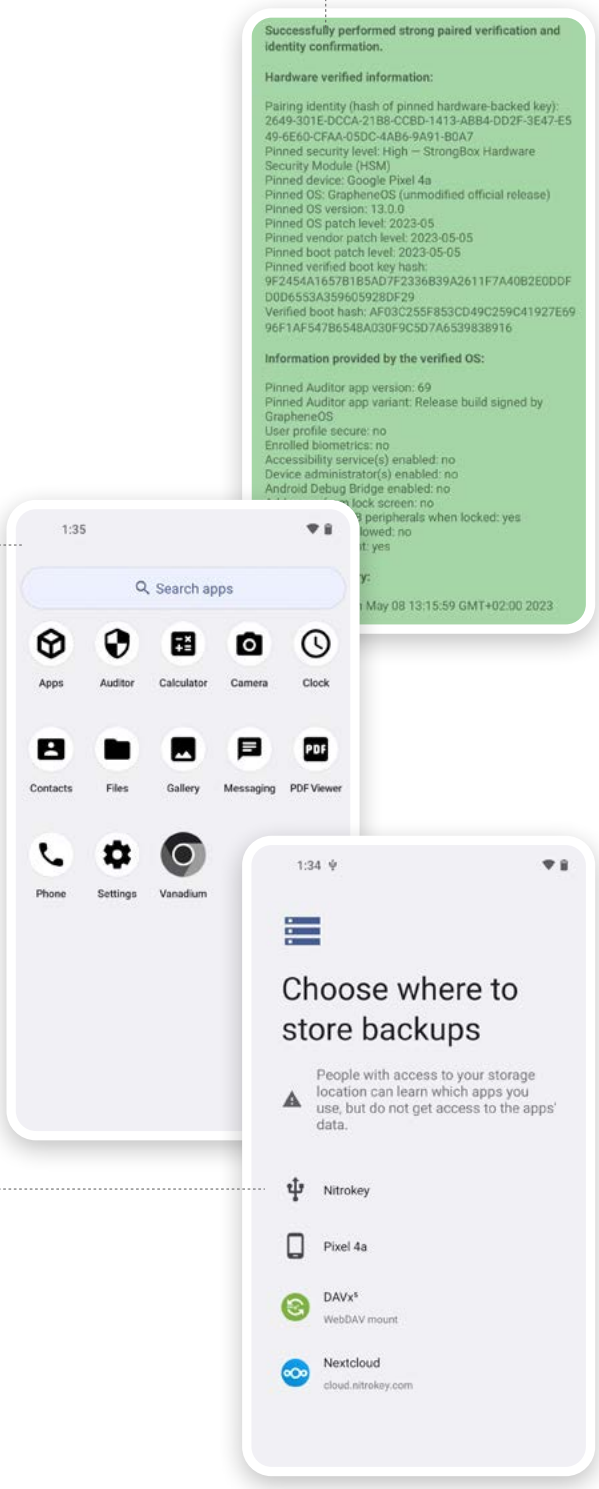
Open Source and Attestation

Checking for backdoors

Open source allows checking for backdoors.

Full control

Hardware-based remote attestation of operating system authenticity and integrity.



Easy Usability for Everybody

No bloatware

Minimal secure system with few apps by default. Additional apps can be installed manually; updates have to be confirmed.

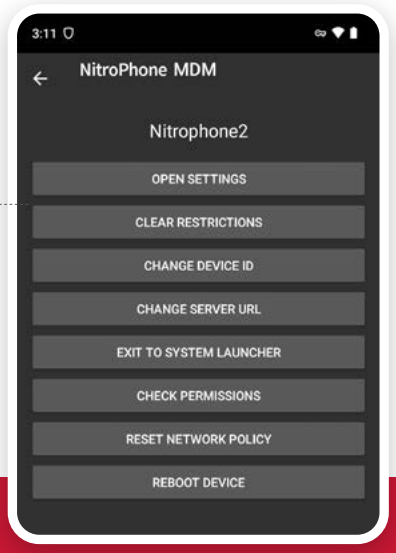
End-to-end encrypted backups

End-to-end encrypted automatic backups to USB drive or to any cloud storage (e.g. Nextcloud).

Enterprise-Ready MDM

Mobile Device Management (MDM)

To manage a larger number of devices and enforce policies and configurations on them, a powerful MDM is available as open source. Organizations can operate it themselves or obtain as a service.



Who Needs NitroPhone and NitroTablet?

People who want to use a privacy-friendly smartphone or tablet (without Google, without Apple).

Companies and authorities who want to provide their employees a secure smartphone or tablet.

Executives, VIPs and professionals who need a secure smartphone or tablet for sensitive data and communication.

Journalists, activists and NGOs who need to protect themselves and their contacts.

www.nitrokey.com

Our Customers

Version: 09/2023