

# NitroPhone, NitroTablet

## Das sicherste Android auf dem Planeten

Das NitroPhone bzw. NitroTablet kombiniert Sicherheit, Privatsphäre und einfache Bedienung mit moderner Hardware. Langfristige Software-Updates von bis zu 7 Jahren garantieren Nachhaltigkeit und einen niedrigen Preis pro Zeit. Das NitroPhone bzw. NitroTablet basiert auf der hochwertigen Pixel-Hardware und GrapheneOS, dem härtesten Android für Privat und Profis.

- ✓ **Sicherheit:** Gehärtetes Android und Hardware-Sicherheit für professionelle Ansprüche.
- ✓ **Datenschutz:** 100% Open Source unter Ihrer Kontrolle ohne Google, Apple und Cloud.
- ✓ **Optional:** Ausbau der Mikrofone, Sensoren, Kameras und Funkmodule machen das Abhören der Umgebung physisch unmöglich. Telefonate werden mit optionalem Headset geführt.

**„NitroPhone ist ein viel besseres Produkt als unser Blackphone.“**

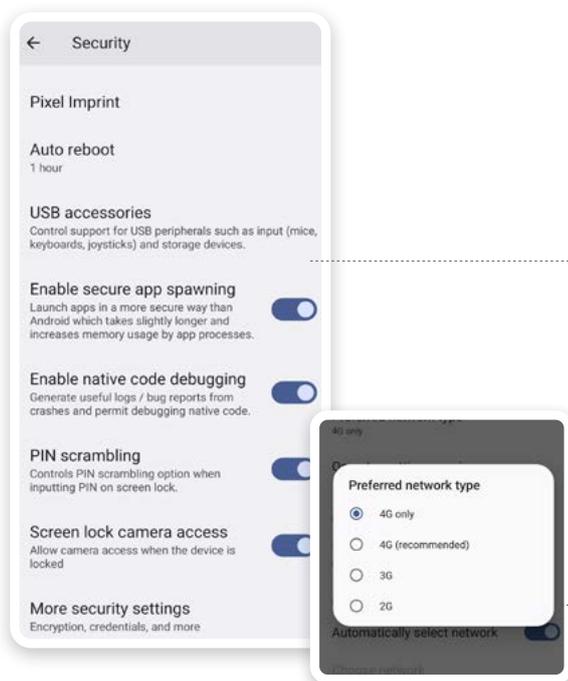
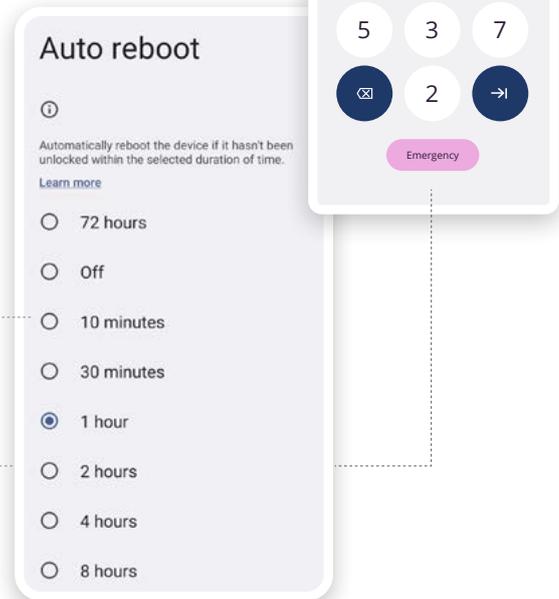
*Phil Zimmermann, Erfinder von PGP*

**„Wenn ich heute ein Smartphone konfigurieren würde, würde ich Daniel Micays GrapheneOS als Basis-Betriebssystem verwenden. Ich würde die Mikrofone auslöten.“**

*Edward Snowden, NSA-Whistleblower*

## Schutz vor physischer Manipulation

- ✓ **Starke Verschlüsselung** und der Titan Sicherheitschip schützen Ihr Gerät und Ihre Daten vor fortgeschrittenen physischen Angriffen.
- ✓ **Verifizierter Boot** stellt sicher, dass Ihr Betriebssystem nicht verändert wurde.
- ✓ **Automatischer Kill Switch:** Automatisches Herunterfahren nach Inaktivität über einen bestimmten Zeitraum.
- ✓ **Verwürfeltes PIN-Layout**, zusammen mit der Blickschutzfolie (nicht enthalten), ermöglicht die Eingabe der PIN in der Öffentlichkeit, ohne beobachtet zu werden. Alternativ: integrierter Fingerabdruck-Sensor.
- ✓ Das NitroPhone bzw. NitroTablet wird im **versiegelten Karton** geliefert.



## Schutz vor Spyware und Zero-Day-Exploits

- ✓ **Stark gehärtetes aktuelles Android** für hohe Sicherheitsanforderungen (z.B. gehärtete Stock-Apps, libc, malloc, Compiler-Toolchain, Kernel, Dateisystemzugriff, WebView).
- ✓ Alle Apps werden in einer **Sandbox** ausgeführt, um vor angreifbaren und bösartigen Apps zu schützen.
- ✓ **Gehärteter Browser**, WebView und PDF-Viewer.
- ✓ **Schutz gegen over-the-air Exploits**, indem der Baseband-Funkprozessor mittels IOMMU isoliert wird und optionaler Nur-LTE-Modus um die Angriffsfläche des Mobilfunks signifikant zu reduzieren.

## Optional: ohne Mikrofone, Sensoren, Kameras, Funkmodule

**Optional:** Für sehr hohe Sicherheitsanforderungen können alle Mikrofone, Kameras sowie Beschleunigungs- und Rotationssensoren ausgebaut werden. Denn Beschleunigungs- und Rotationssensoren könnten als Mikrofone missbraucht werden. Somit wird physisch verhindert, dass Gespräche in der Umgebung belauscht werden können. Telefonate können trotzdem mit externem Headset geführt werden. Beim NitroTablet können zusätzlich alle Funkmodule ausgebaut werden.



# Schutz der Privatsphäre: Kein Tracking, kein Google

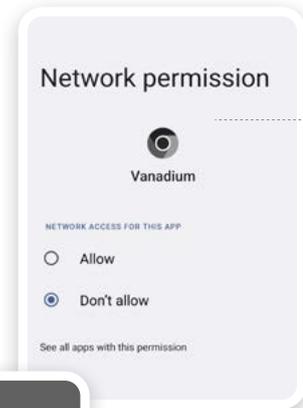
✓ **Standardmäßig keine Integration von Cloud oder Google Play Services**, alles unter Ihrer Kontrolle. Bei Bedarf können die originalen Google Play Services in einer Sandbox ohne besondere Privilegien installiert werden. Dieser neuartige Ansatz führt zu deutlich besserer Kompatibilität als unvollständige Neuimplementierungen wie microG bei gleichzeitig höherer Sicherheit.

✓ **Schutz vor Tracking:** Apps können nicht auf IMEI- und Seriennummern des Gerätes, Seriennummern der SIM-Karte, Teilnehmer-ID, MAC-Adresse usw. zugreifen.

✓ Die MAC-Randomisierung pro Verbindung **verhindert die Verfolgung (Tracking)** durch WiFi-Scanner in der Nähe.

✓ **Firewall:** Granulare Netzwerk- und Sensor-Berechtigungen (z.B. GPS) für jede App einstellbar.

✓ **Standardindikatoren** für aktive Kamera, Mikrofon und Standortlokalisierung.



## Sichere Kommunikation

✓ Für sichere Nachrichten, Sprach- und Videoanrufe nutzen Sie das kostenlose, Ende-zu-Ende-verschlüsselte und **datenschutzfreundliche Signal und NitroChat**. Alternativ unterstützen wir Sie beim Betrieb eines eigenen Matrix-Servers.



Auswahl

## MODERNE HARDWARE

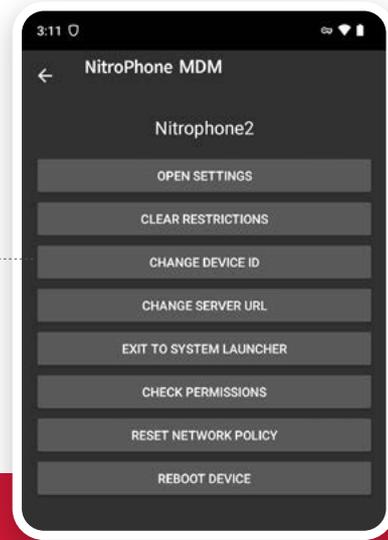
Das NitroPhone gibt es in unterschiedlichen Ausführungen zwischen moderner Mittelklasse- und Highend-Niveau. Zudem ist es auch als großformatiges NitroTablet verfügbar.



# MDM für Unternehmen

## + Geräteverwaltung

Um eine größere Anzahl an Geräten zu verwalten und Richtlinien und Konfigurationen auf diesen umzusetzen, steht ein leistungsfähiges Mobile Device Management (MDM) als Open Source zur Verfügung. Organisationen können dies selber betreiben oder als Service beziehen.



## Wer benötigt NitroPhone bzw. NitroTablet?

**Menschen**, die ein Datenschutz-freundliches Smartphone bzw. Tablet (ohne Google, ohne Apple) nutzen wollen.

**Firmen und Behörden**, die Ihren Mitarbeitern ein sicheres Smartphone bzw. Tablet zur Verfügung stellen möchten.

**Führungskräfte, VIPs und Profis**, die ein sicheres Smartphone bzw. Tablet für sensible Daten und Kommunikation benötigen.

**Journalisten, Aktivisten und NGOs** die sich und Ihre Kontakte schützen müssen.

[www.nitrokey.com](http://www.nitrokey.com)

## Unsere Kunden

Stand: 10/2024

