



# Smarte Technologien und die Sicherheit

Ralf Benzmüller  
Leiter G Data SecurityLabs

G Data. Security **Made in Germany.**



## Agenda

- Smartphones: Android Malware
- Smart TV
- Smart Homes
- Smart Cars
- Smart Energy

G Data. Security **Made in Germany.**



# ANDROID !



G Data. Security **Made in Germany.**



# Telefone vor ein paar Jahren



Quelle: openclipart.org

G Data. Security **Made in Germany.**



## Telefone heute



Quelle: openciptart.org

G Data. Security **Made in Germany.**

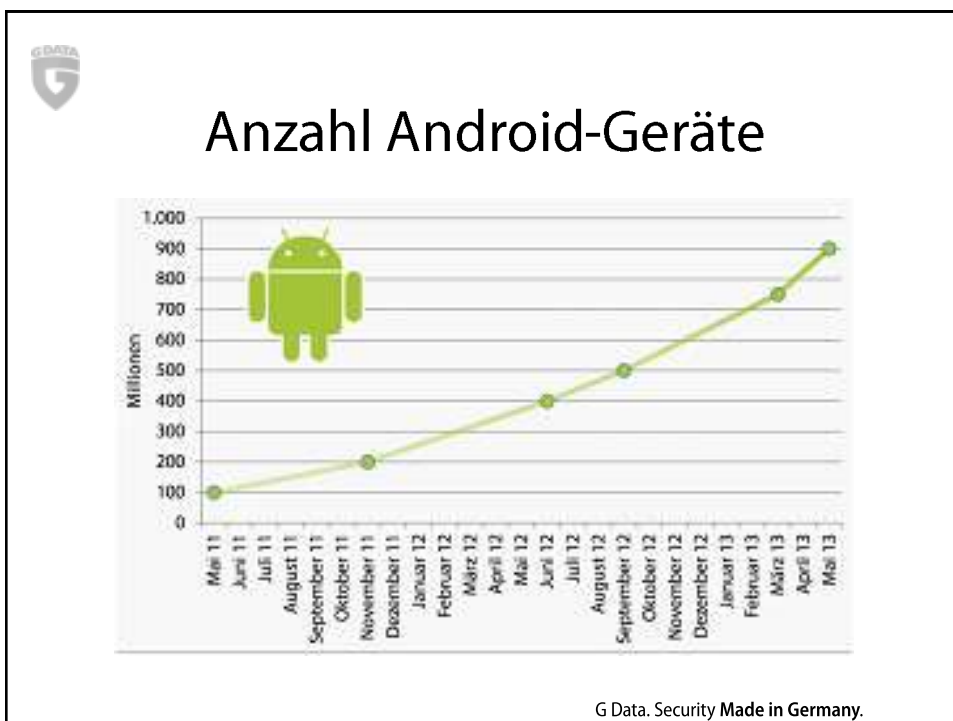
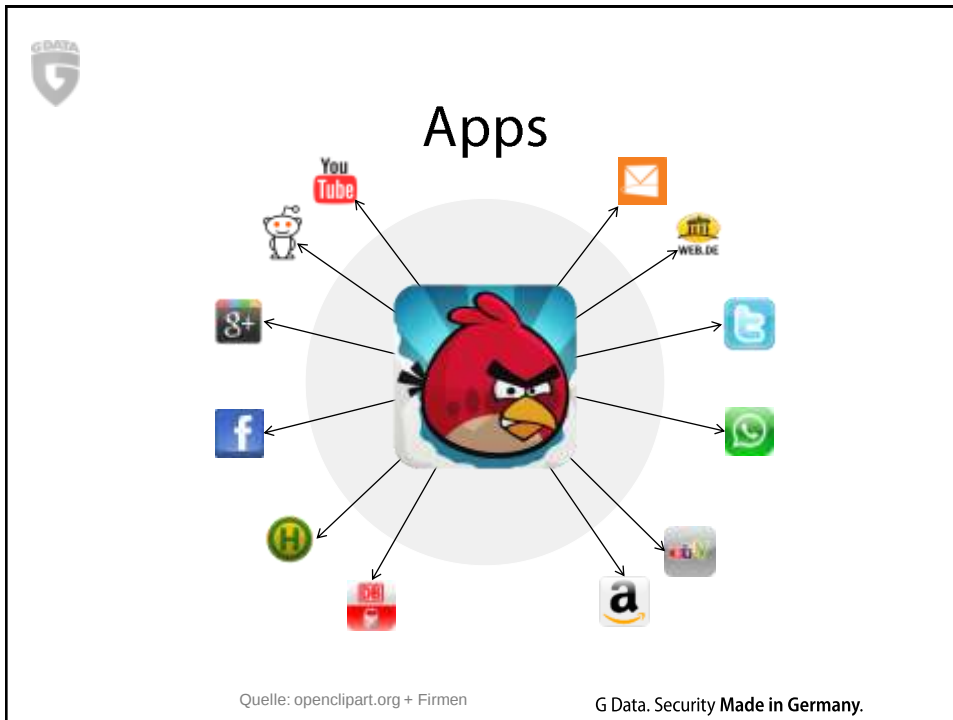


## Apps



Quelle: openciptart.org + Firmen

G Data. Security **Made in Germany.**





# Wo ist der Unterschied



G Data. Security Made in Germany.





# Dalvik

- Dalvik ist nicht Java!
  - 1) Man schreibt Code in... Java
  - 2) Kompiliert ihn mit Java Compiler...
  - 3) Und wandelt ihn in Dalvik Bytecode...



<http://maps.google.de/>

G Data. Security **Made in Germany.**



# Dalvik VM

- Register basiert
- Optimiert für geringen Speicherverbrauch
- Optimiert für langsame CPUs
- Kein Swap-Space
- Kein JIT

G Data. Security **Made in Germany.**



## Exkurs – Sicherheit Android

- Unix multi-user Sandbox (uid/gid)
- Jede App hat eigene ID

```
# ls -l /data/data/
drwxr-x--x app_36 app_36 2011-06-27 13:51 de.gdata.mobilesecurity
drwxr-x--x app_0 app_0 2011-06-27 11:02 com.android.providers.applications
drwxr-x--x app_1 app_1 2011-06-27 11:02 com.android.speechrecorder
drwxr-x--x app_3 app_3 2011-06-27 11:03 com.android.inputmethod.latin
drwxr-x--x app_4 app_4 2011-06-27 11:03 com.android.customlocale
drwxr-x--x app_0 app_0 2011-06-27 11:03 com.android.inputmethod.pinyin
drwxr-x--x system system 2011-06-27 11:03 com.android.providers.subscribedfeeds
drwxr-x--x app_2 app_2 2011-06-27 11:03 com.android.providers.drm
drwxr-x--x app_5 app_5 2011-06-27 11:03 com.android.cardlock
```

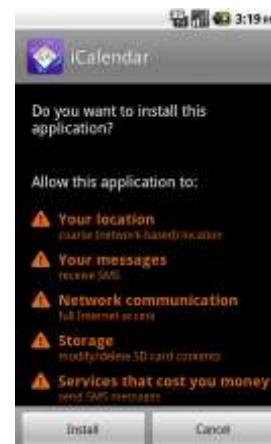
- Entwickler können IDs teilen

G Data. Security Made in Germany.



## Exkurs – Sicherheit Android

- Keine Rechte per default
- Rechtevergabe
  - Durchgesetzt vom Kernel
  - Angezeigt bei der Installation
  - Unveränderbar
- Apps sind signiert



G Data. Security Made in Germany.



## Android Malware 2010

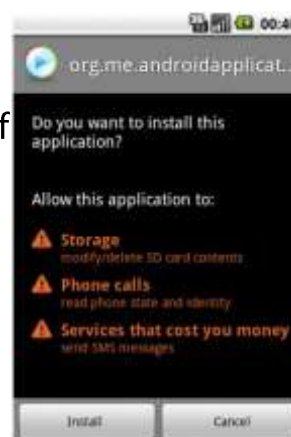
- 2010.08 **Fakeplayer**
- 2010.12 **Geinimi**



## 2010.08 Fakeplayer



- 1. SMS Trojaner
- Versendet Premium-SMS
- Deaktiviert sich nach erstem Lauf
- 8+ Varianten
  - Verschiedene Namen/Icon
    - „Porno Player“
    - „Pornplayer“
    - „Video Player“
  - Verschiedene SMS Nummern



G Data. Security Made in Germany.

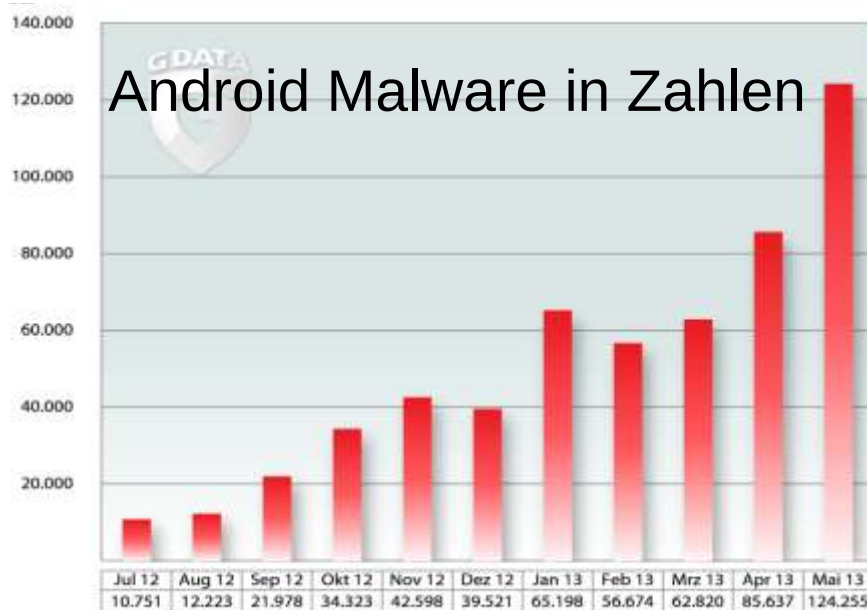


## 2010.12 Geinimi

- 1. Botnetz => SMS, Anrufe
- Obfuscation & Krypto
- Datendiebstahl
  - IMEI, IMSI, GPS, Telefonnummer
- 24 infizierte Apps



G Data. Security Made in Germany.



G Data. Security Made in Germany.



## Android Malware 2013 H1

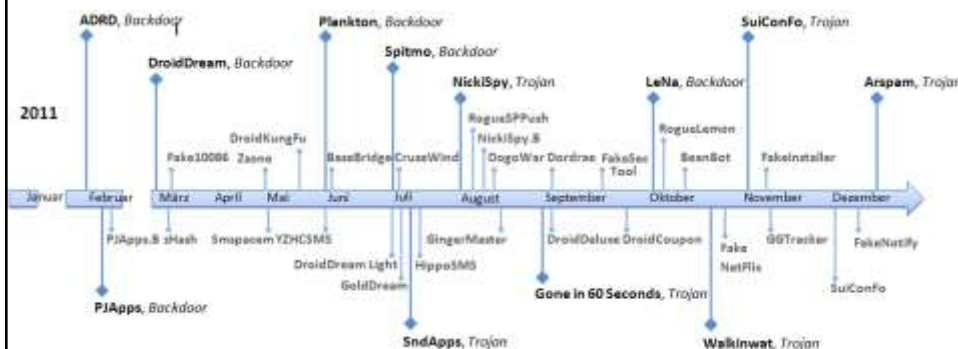
- 519.095 neue Schaddateien
- 16 mal mehr als im Jahr zuvor
- 454 Familien, 1919 Varianten

| Familie               | # Varianten |
|-----------------------|-------------|
| Trojan.Agent          | 266         |
| Trojan.FakeInstaller  | 168         |
| Backdoor.GingerMaster | 156         |
| Trojan.SMSAgent       | 100         |
| Trojan.SMSSend        | 92          |

G Data. Security Made in Germany.



## Android Malware 2011

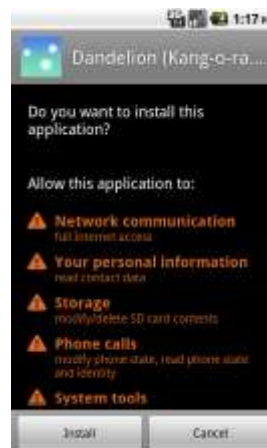


G Data. Security Made in Germany.



## 2011.02 **ADRD**

- Botnetz
- Animiertes Hintergrundbild
  - Taucht nicht im Launcher auf
- SEO auf baidu.com
  - Wechselt sogar zwischen Wifi/3G/...

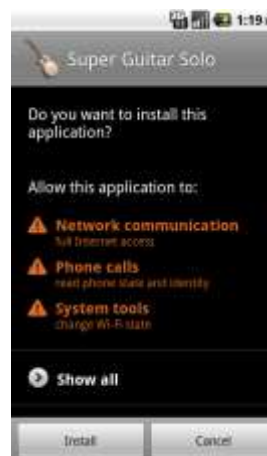


G Data. Security Made in Germany.



## 2011.03 **DroidDream**

- Botnetz
- 2x Exploits dabei
  - Root Shell für C&C (#1)
  - Läuft als Dienst mit Root rechten
- Erste Malware im Android Market
  - 50+ Apps
  - 250k+ Infektionen



G Data. Security Made in Germany.



## 2011.06 Plankton

- Botnetz
- Update
  - Lädt erlaubte Rechte hoch (AndroidManifest.xml)
  - Lädt spezifischen Code runter
  - Führt diesen dynamisch aus



G Data. Security Made in Germany.



## ZITMO, SPITMO CITMO

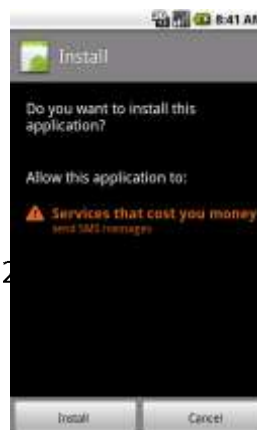
- **Z**eus **I**n **T**he **M**obile (**S**PyEye, **C**arberp)
- Banking-Trojaner leiten SMS mit MTAN an Cyberdiebe weiter
- Symbian, iOS, Blackberry, Android

G Data. Security Made in Germany.



## 2011.11 FakeInstaller

- SMS Trojaner
- Versendet Premium-SMS
- Meta-Installer für Skype, Opera, ...
- Ist aktuell die produktivste Familie
  - 31% aller Schaddateien im 1. Hj. 2013
  - ~70% aller Schaddateien im 2. Hj. 2012



G Data. Security Made in Germany.



Tools:

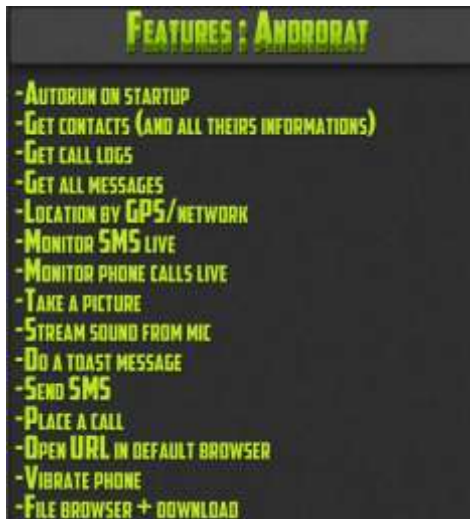


**ANDRORAT APK BINDER IS AN ANDROID APP BINDER MADE SPECIFICALLY FOR USE WITH THE FREE OPEN SOURCE ANDROID RAT "ANDRORAT". IT WORKS BY DECOMPILING ANY LEGIT ANDROID APP, RE-WRITING THE ANDRORAT CLIENT SOURCE TO INCLUDE YOUR IP + PORT, AND THEN INJECTING ANDRORAT INTO THE DECOMPILED APP. ONCE REBUILT, YOU ARE LEFT WITH A FULLY FUNCTIONING REAL APP THAT ALSO CONTAINS YOUR ANDRORAT TROJAN!**

G Data. Security Made in Germany.



## Tools: Androrat



OpenSource Projekt

G Data. Security Made in Germany.



## Tools: Androrat APK Binder



G Data. Security Made in Germany.



## Tool: APK-Binder



G Data. Security Made in Germany.



## 2011.11 SuiConFo

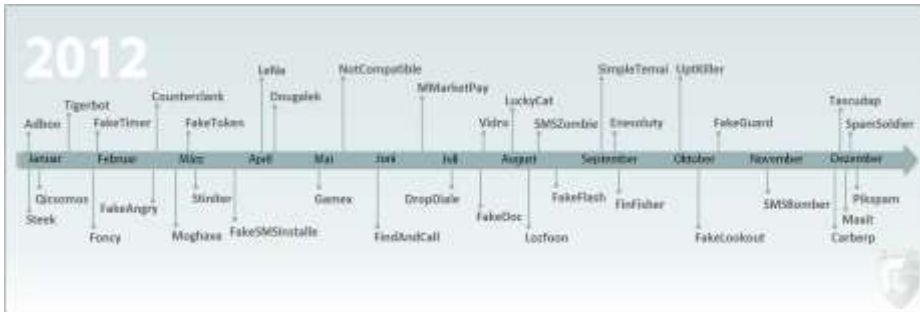
- SMS Trojaner
- Versendet Premium-SMS
- Zeigt Fehlermeldung
- Erstmals mit länder-spezifischen Rufnummern



G Data. Security Made in Germany.



## Android Malware 2012



G Data. Security Made in Germany.



## FakeDoc

- Batterie App
- Installiert einen Push-Service, der Werbung einblendet
- Die Werbung bleibt auch, wenn die Original-App deinstalliert wurde



G Data. Security Made in Germany.



## FindandCall.A



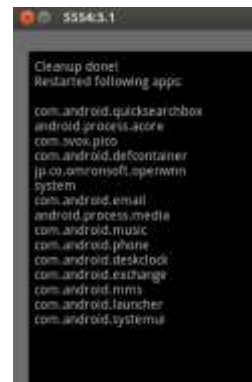
- Sendet Kontaktdaten an Server
- Server versendet SMS-Spam an Kontakte (auch Links zu Malware)
- Trotz Google Bouncer im Google Play Store verfügbar

G Data. Security Made in Germany.



## SuperClean

- Cross Plattform Malware
  - Infiziert Windows Rechner
- Botnetz
  - Anrufe durchführen
  - SMS löschen
  - Stiehlt Dateien/SMS/Kontakte/Bilder
  - Dropbox Phishing

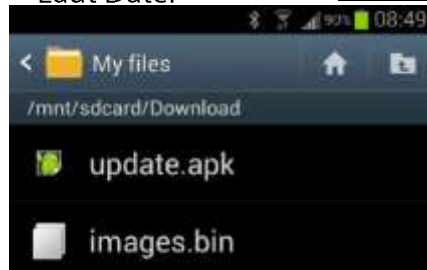
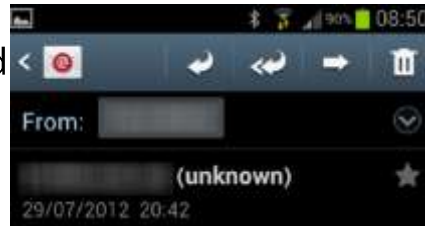


G Data. Security Made in Germany.



## 2012.05 NotCompatible.A

- 1. Drive-By-Download
- E-Mail von Yahoo
- Link zu Webseite
  - Lädt Datei



G Data. Security Made in Germany.



## 2012.10 FakeLookout



Quelle: <http://blog.trustgo.com/fakelookout/>

G Data. Security Made in Germany.



## 2012.10 FakeLookout

- Tut nichts
- Dienst reagiert auf viele Intents
- Kontaktiert C&C Server
- Liste der Befehle

| bt_value                            |
|-------------------------------------|
| java/lang/StringBuilder->toString() |
| "clearFileList"                     |
| "clearFileList"                     |
| "getDir"                            |
| "clearAlarm"                        |
| "clearAlarm"                        |
| "getTexts"                          |
| "GotTexts"                          |
| "getFile"                           |
| java/lang/StringBuilder->toString() |
| "getSize"                           |

Quelle: <http://blog.trustgo.com/fakelookout/>

G Data. Security Made in Germany.



## Was tut Android Malware?

- Daten stehlen
  - Gerät, Nutzer, Kontakte, SMS, Anrufe, Location, Banking, Zugangsdaten
- SMS versenden, überwachen, filtern
- Adware, FakeAV
- Apps kaufen
- WAP-Spiele spielen
- Politische Botschaften verbreiten

G Data. Security Made in Germany.



## Was tut Android Malware?

- Botnetz (C&C auch per SMS, Twitter)
- Download & Install
- Geräte rooten
- Ratings manipulieren
- Selbstschutz: Kill AV, keine Icon, Uninstall--
- Monitoring Tools, Riskware
- Daten zerstören

G Data. Security Made in Germany.



## Fazit

- Android Malware ist professionell
  - Premium-SMS, Werbung, SMS-Spam
  - Robocalls, Datendiebstahl
- Android Malware ist etabliert
- Die Infrastruktur zur kriminellen Verwertung entsteht gerade
- Ein Virenschutz ist notwendig!

G Data. Security Made in Germany.



# Agenda

- Smartphones: Android Malware
- Smart TV
- Smart Homes
- Smart Cars
- Smart Energy

G Data. Security **Made in Germany.**



## Smart TV

- Android TV => s.o.
- HBB TV (Hybrid Broadcasting Broadband)
  - Kombiniert Internet und DVB-Empfang
  - Zusatzinfos sollen Teletext ersetzen
  - Webseite als Overlay zum User tracking
    - Red Button ruft Daten von Webserver des Senders ab
    - URL im Sendesignal manipulieren
    - DNS-Spoofing

G Data. Security **Made in Germany.**



## Smart TV oder Televisor?

- Samsung Smart TV (Grattafiori & Yavor, 2013)
  - Nur ein Nutzer: „root“ => ein Exploit reicht
  - Mangelhafte TLS-Zertifikatsprüfung
  - Kontrolle über Kamera und Mikrofon
  - Zugriff auf Daten
  - Zugriff auf Rechenleistung

G Data. Security Made in Germany.



## Agenda

- Smartphones: Android Malware
- Smart TV
- Smart Homes
- Smart Cars
- Smart Energy

G Data. Security Made in Germany.



## Smart Homes im Internet der Dinge

- Steuerung von
  - Heizung, Gas, Wasser
  - Pumpen und Ventile
  - Licht
  - Garagentor
  - Fernseher
  - Kameras
  - Schließanlagen

G Data. Security Made in Germany.



## Smart Homes – status quo

- Insteon
  - Steuerung per App ohne Authentifizierung
  - Google Suche zeigt falsch konfigurierte Systeme an

G Data. Security Made in Germany.



## Smart Homes – status quo

- Vaillant eco Power 1.0
  - Nano Blockheizkraftwerke für 1-2 Familienhäuser
- Web-Interface zur Fernsteuerung durch Besitzer und Service-Personal
- Anlagen melden sich bei DynDNS-Dienst von Vaillant an
  - Durch Probieren kann man auf Systeme zugreifen

G Data. Security Made in Germany.



## Smart Homes – status quo

- Lösung von Vaillant
  - Kunden per Post informiert
  - Netzwerkstecker ziehen !!!
  - Kundendienst kommt und fixt
  - VPN nur für Kunden mit Wartungsvertrag kostenlos

G Data. Security Made in Germany.



# Agenda

- Smartphones: Android Malware
- Smart TV
- Smart Homes
- Smart Cars
- Smart Energy

G Data. Security **Made in Germany.**



## SmartCars

- Grundproblem CAN (Controller Area Network)
- Zugriff auf CAN Bus per OBD-II  
(Fahrzeugdiagnose, in USA gesetzlich vorgeschrieben)
- Trennung der Netze von  
Kernfunktionen und Infotainment
- Authentifizierung, Signierung

G Data. Security **Made in Germany.**



## Car Hacking – Miller & Valasek

- Toyota Prius, Ford Escape (2010)
- Fahrassistenzsysteme inklusive
  - Einparkhilfe
- Hack vom Rücksitz
  - Bremsen und Lenkrad kontrollieren
  - Licht, Radio, Strom an/aus
  - Manipulation der Anzeigen

G Data. Security Made in Germany.



## Car Hacking

- Voraussetzungen
  - Nähe
  - Physikalischer Zugriff
  - Paket-Sniffing
- Aber:
  - Funkangriffe per Buffer Overflow in Bluetooth-Modul
  - Standard-PINs

G Data. Security Made in Germany.



# Agenda

- Smartphones: Android Malware
- Smart TV
- Smart Homes
- Smart Cars
- Smart Energy

G Data. Security **Made in Germany.**



## Smart Energy

- Energiewirtschaftsgesetz
- Einführung ab 2014
  - Pflicht bei Neubauten und Verbraucher, mit mehr als 6000 KWh/Jahr
  - 80% bis 2020, total 2029
- Hohe Sicherheitsanforderungen

G Data. Security **Made in Germany.**

