Keamanan Seluler, Aplikasi, dan IoT

Protecting data and devices worldwide

Peningkatan signifikan serangan siber yang disponsori negara dan pelaku kejahatan di dunia maya membuat kami percaya bahwa produk dan layanan kami hanya akan berguna jika aman. Di Google, kami semakin memfokuskan tujuan kami untuk melindungi masyarakat, organisasi, dan pemerintah dengan membagikan keahlian kami, memberdayakan masyarakat untuk mengatasi risiko siber yang terus berkembang, dan terus berupaya memajukan kecanggihan dalam keamanan siber untuk membangun dunia yang lebih aman bagi semua orang.

Oleh karena itu, kami harus tetap menjadi yang terdepan dan terus mengembangkan solusi keamanan kami guna mengatasi lanskap ancaman yang terus berkembang, terutama dalam hal mengamankan semua perangkat dan aplikasi yang terhubung, demi menyediakan lingkungan yang aman bagi konsumen di mana mereka memiliki kebebasan dan pilihan atas perangkat yang mereka gunakan.

Tantangan

Ada harga, ada konektivitas

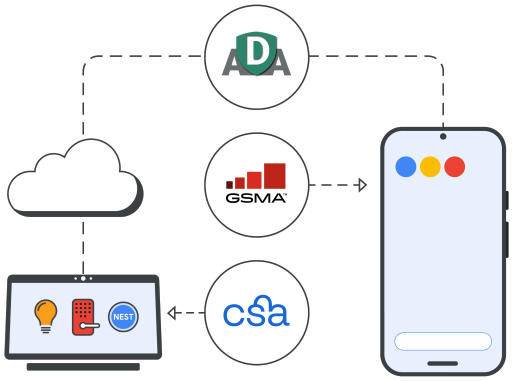
Kita melakukan berbagai aktivitas dalam kehidupan sehari-hari menggunakan ponsel pintar, aplikasi, dan perangkat IoT—menghabiskan lebih banyak waktu secara online, dan dalam prosesnya, berbagi lebih banyak data berharga, seperti informasi perbankan atau perawatan kesehatan. Akibatnya, penjahat siber yang canggih semakin menargetkan perangkat ini lebih dari sebelumnya guna mendapatkan informasi sensitif.

Lebih banyak perangkat, lebih banyak data–lebih banyak ancaman

Saat ini diperkirakan ada sekitar 17 miliar perangkat IoT di dunia, mulai dari printer hingga pembuka pintu garasi, masing-masing dilengkapi perangkat lunak (beberapa di antaranya merupakan sumber terbuka) yang dapat dengan mudah diretas.[1] Secara umum, jumlah perangkat IoT yang disusupi hampir mencapai dua kali lipat pada tahun 2020.[2]

- Meskipun perangkat IoT membantu kita menjadi semakin terhubung, tidak ada standar global untuk mengukur kualitas keamanan produk yang terhubung sehingga konsumen tidak dapat mengambil keputusan terkait keamanan perangkat tanpa informasi yang memadai.
- Konsumen seharusnya memiliki hak untuk mendapatkan transparansi terkait produk digital yang mereka miliki, seperti halnya mereka memiliki hak untuk mengetahui bahan-bahan apa saja yang terkandung di dalam makanan atau bahan pembersih yang mereka beli.
- Perangkat seluler hanya merupakan satu titik masuk ke pintu serangan lain, dan interkonektivitas perangkat meningkatkan kebutuhan akan transparansi keamanan dalam skala besar. Oleh karena itu, keamanan ekosistem perangkat yang terhubung sama pentingnya dengan keamanan jaringan dan sistem.

Kolaborasi kami dengan organisasi industri



Solusi Kami

Di Google, kami memajukan keamanan dan transparansi perangkat yang terhubung melalui keamanan seluler, aplikasi, dan IoT:

Keamanan Seluler

Android, sistem operasi sumber terbuka kami, memanfaatkan pendekatan keamanan berlapis untuk menjaga keamanan perangkat seluler:

- Keamanan Berlapis
  - Boot Terverifikasi, perlindungan roll-back, dan perlindungan pengaturan ulang pabrik memastikan versi Android terkini dan teraman.
  - PIN dan autentikasi biometrik melindungi perangkat dari akses luar.
  - 'Temukan Perangkat Saya' membantu menemukan perangkat atau menghapus data di dalamnya jika perangkat dicuri atau hilang.
- Perlindungan identitas dan kata sandi
  - Verifikasi 2 Langkah, Ponsel sebagai Kunci Keamanan, dan Pengelola Kata Sandi melindungi akun Google Anda dari akses pihak luar.
  - Pemeriksaan keamanan dan Perlindungan Lanjutan opsional menjaga perangkat tetap berjalan dengan aman dan lancar.
- Perlindungan anti-phishing
  - Phone by Google dan Messages by Google membantu mendeteksi dan mencegah serangan penipuan dan phishing.
  - Penjelajahan Aman Google melindungi lebih dari 5 miliar perangkat secara global.

Keamanan Aplikasi

Anti-malware unik membantu mencegah aplikasi berbahaya dan memberikan transparansi informasi keamanan data kepada pengguna saat mengunduh aplikasi.

- Google Play Store: Alat pendeteksi pembelajaran mesin dan analis manusia meninjau semua aplikasi sebelum tersedia untuk diunduh. Bagian Keamanan Data menjelaskan jenis data yang dikumpulkan aplikasi dan untuk apa data tersebut digunakan.
- Google Play Protect: Memindai lebih dari 125 miliar aplikasi setiap hari dan memberi tahu, menghapus, atau menonaktifkannya jika risiko keamanan terdeteksi.
- App Defense Alliance (ADA): Google bekerja sama dengan mitra pendeteksi ancaman seluler terkemuka untuk meluncurkan App Defense Alliance yang membantu melindungi pengguna Android dari Aplikasi yang Berpotensi Membahayakan (Potentially Harmful Applications/PHA) melalui informasi bersama dan deteksi yang terkoordinasi.

Keamanan IoT

Label keamanan IoT dengan jelas menyampaikan praktik privasi dan keamanan pada perangkat, misalnya data apa saja yang dikumpulkan.

- Kami percaya pada lima prinsip inti untuk Skema pelabelan keamanan IoT: label langsung, skema evaluasi, dasar keamanan yang digabungkan dengan fleksibilitas, transparansi menyeluruh, dan insentif adopsi.
- Kami bekerja sama dengan Aliansi Standar Konektivitas/Connectivity Standards Alliance (CSA) dan Aliansi GSM (GSMA) untuk menstandardisasi program sertifikasi di seluruh industri untuk persyaratan peraturan yang ada dan yang akan datang.

Prinsip Kami

Di Google, kami menerapkan 3 prinsip utama untuk memajukan keamanan dan transparansi perangkat yang terhubung:

Defense in Depth: Kami menggunakan arsitektur keamanan berlapis yang bekerja sama untuk membangun pertahanan kuat yang berjalan tanpa hambatan dan efektif.

Open & Transparent: Transparansi adalah kunci filosofi kami. Dengan memberikan informasi kepada pengguna platform kami dan berbagi pengetahuan untuk meningkatkan perlindungan kami, kami percaya bahwa ekosistem sumber terbuka dapat menjadi lebih aman dari sumber tertutup.

Yang terbaik dari Google dan Ekosistem kami: Kami bermitra dengan tim ahli di seluruh Google dan industri untuk membantu menjaga keamanan miliaran pengguna.

Aplikasi

Label keamanan IoT: meletakkan kendali di tangan konsumen

Tanpa pelabelan keamanan IoT yang solid, tidak ada standar global yang dapat diikuti oleh produsen perangkat. Pengguna juga tidak memiliki visibilitas yang layak untuk mengetahui apakah perangkat tersebut melindungi data mereka. Industri ini perlu bersatu untuk mengedepankan keamanan IoT dan mengembalikan kendali ke tangan konsumen. Kami sedang mengerjakan skema pelabelan keamanan IoT melalui proses dan kemitraan kami.

Pertama, kami berinvestasi dalam penelitian keamanan di luar Google untuk menunjukkan kemungkinan kerentanan (Google Nest berpartisipasi dalam program penghargaan kerentanan Google dan memberikan hadiah bagi peneliti keamanan di luar Google yang menemukan kerentanan). Kemudian, kami mengeluarkan patch dan perbaikan bug yang penting selama setidaknya lima tahun setelah peluncuran.

Semua perangkat kami yang dikembangkan pada tahun 2019 dan selanjutnya menggunakan Boot Terverifikasi untuk memastikan perangkat lunak yang tepat beroperasi dan aksesnya terlindungi. Misalnya, perangkat Google Nest kami divalidasi menggunakan standar keamanan pihak ketiga yang diakui industri, seperti yang dikembangkan oleh NIST, ETSI, dan ISO.

Standar-standar ini, dan Siklus Hidup Pengembangan Perangkat Lunak (Software Development Life Cycle/SDLC) kami yang aman, mengurangi kemungkinan konsumen terpapar praktik keamanan yang buruk dan membuka jalan bagi internet yang terbuka dan lebih aman.

Investasi dan pencapaian industri kami

2007 Menetapkan Penjelajahan Aman untuk secara proaktif memperingatkan pengguna ketika mereka mengunjungi situs web berbahaya, yang sekarang melindungi lebih dari 5 miliar perangkat.

2010 Meluncurkan Laporan Transparansi Google untuk menunjukkan bagaimana kebijakan serta tindakan pemerintah dan perusahaan memengaruhi privasi, keamanan, dan akses ke informasi online. Pada tahun 2018, kami menambahkan Laporan Transparansi khusus Android.

2017 Meluncurkan Google Play Protect yang kini menjadi solusi anti-malware yang paling banyak digunakan dan memindai lebih dari 125 miliar aplikasi per hari di lebih dari 3 miliar perangkat.

2019 Mengenalkan Kunci Keamanan sebagai fitur bawaan di Android dan kemudian untuk iPhone pada tahun 2020.

2022 Google Play meluncurkan bagian keamanan data untuk memberikan lebih banyak informasi kepada masyarakat tentang bagaimana aplikasi mengumpulkan, membagikan, dan mengamankan data pengguna serta memprakarsai sistem lencana pertama untuk aplikasi apa pun yang telah menyelesaikan tinjauan keamanan terpisah melalui App Defense Alliance.

2023 Passkey: masa depan tanpa kata sandi sedang diluncurkan dengan dukungan passkey yang diperluas setelah satu dekade mendorong standar terbuka dengan Aliansi FIDO dan para pemimpin teknologi di seluruh dunia.

Pendekatan Kami

Berkomitmen pada dunia digital yang terbuka dan aman

Masalah keamanan akan semakin meningkat dengan semakin banyaknya data di lebih banyak perangkat di jaringan yang berbeda. Kami membantu memajukan masa depan keamanan perangkat terhubung melalui pengembangan produk, kriteria transparansi, dan kemitraan industri kami

Landasan strategi produk kami adalah memastikan produk kami aman secara default. Penjelajahan Aman, Google Play Protect, dan Kunci Keamanan bawaan melindungi perangkat seluler dan aplikasi untuk memberikan tingkat keamanan tertinggi pada produk kami.

Kami membantu mendemokratisasi operasi keamanan dengan bersikap terbuka dan transparan dalam menangani masalah dan berbagi pengetahuan keamanan perangkat yang terhubung. Kami percaya bahwa ekosistem sumber terbuka bisa lebih aman daripada ekosistem sumber tertutup dengan pendekatan keamanan berlapis kami.

Dengan berkolaborasi bersama CSA, ADA, dan GSMA, kami berusaha untuk memajukan teknologi keamanan siber demi masa depan internet yang lebih aman bagi semua pihak.

Kami berkomitmen untuk meningkatkan standar keamanan perangkat yang terhubung dan menetapkan standar untuk lingkungan online yang lebih aman bagi semua orang, di mana saja. Pelajari lebih lanjut tentang kemajuan Google dalam keamanan perangkat terhubung: g.co/connecteddevicesafety

Sumber: [1] CNBC Cyber Report, 9 Januari 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, 20 Juli 2021