

Sécurité des appareils mobiles, des applications et de l'loT (Internet of Things - désigne notamment les objets connectés)

Protéger les données et les appareils dans le monde entier

Face à la montée en flèche des cyberattaques soutenues par certains États et autres acteurs malveillants, nous sommes convaincus que la sûreté de nos produits et services est tout aussi importante que leur utilité. Chez Google, nous sommes plus que jamais mobilisés pour **protéger** les personnes, les organisations et les gouvernements en partageant notre expertise, en **donnant à la société les moyens** de faire face à des risques cyber en constante évolution et en travaillant à faire **progresser** l'état de l'art en matière de cybersécurité afin de construire **un monde plus sûr pour tous**.

Nous devons donc garder une longueur d'avance et faire évoluer en permanence nos solutions de sécurité face à des menaces en constante progression. Nous pourrions ainsi sécuriser tous les appareils connectés et les applications, et offrir aux consommateurs un environnement sûr dans lequel ils pourront choisir en toute connaissance de cause les appareils qu'ils utilisent.

Le défi

La connectivité a un prix

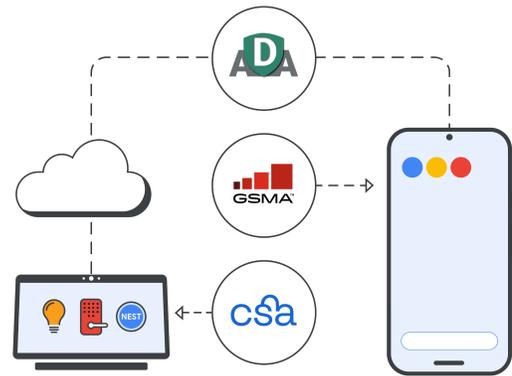
Une part importante de notre vie quotidienne est gérée à partir de nos smartphones, de nos applications et de nos appareils loT. Nous passons de plus en plus de temps en ligne et nous partageons un nombre toujours croissant de données précieuses, telles que des informations bancaires ou relatives à la santé. C'est pourquoi des cybercriminels aux techniques sophistiquées ciblent plus que jamais ces appareils pour obtenir des informations sensibles.

Plus d'appareils et plus de données, donc plus de menaces

On estime aujourd'hui à **17 milliards le nombre d'appareils loT** dans le monde, des imprimantes aux dispositifs d'ouverture à distance de portes de garages, tous équipés d'un logiciel (dont des logiciels open source) pouvant être facilement piratés.¹ Parmi eux, le nombre d'appareils loT compromis a presque **doublé en 2020**.²

- ✓ Alors que nous sommes de plus en plus connectés grâce aux appareils loT, l'absence de normes mondiales permettant de mesurer l'ampleur de la vulnérabilité de ces appareils empêche les consommateurs de prendre des décisions éclairées en matière de sécurité des appareils.
- ✓ Tout comme ils ont accès à la composition des aliments ou des produits de nettoyage qu'ils achètent, les consommateurs devraient avoir le droit à davantage de transparence concernant leurs produits numériques.
- ✓ Les appareils mobiles ne représentant qu'une des portes d'entrée pour d'autres types de menaces, l'interconnectivité des appareils accroît de manière très importante le besoin de transparence en matière de sécurité. C'est pourquoi la sécurité de l'écosystème des appareils connectés est aussi importante que la sécurité des réseaux et des systèmes.

Notre collaboration avec des organisations professionnelles du secteur des télécommunications



Notre solution

Chez Google, nous améliorons la sécurité et la transparence de nos appareils connectés grâce à la sécurité des appareils mobiles, des applications et de l'loT :

Sécurité des mobiles

Android, notre système d'exploitation open source, s'appuie sur une approche de sécurité multicouche pour assurer la sécurité des appareils mobiles :

- ✓ **Sécurité multicouche**
 - La technologie Verified Boot, la protection anti-retour et la protection contre la réinitialisation d'usine garantissent l'utilisation de la version la plus récente et la plus sûre d'Android.
 - L'authentification biométrique et par code PIN protège contre des intrusions extérieures.
 - La fonction « Localiser mon appareil » permet de localiser l'appareil ou de le vider de ses données en cas de vol ou de perte.
- ✓ **Protection de l'identité et du mot de passe**
 - La vérification en 2 étapes, l'utilisation du téléphone comme clé de sécurité et le gestionnaire de mots de passe protègent votre compte Google contre les intrusions extérieures.
 - Le contrôle de sécurité et la protection avancée en option permettent à l'appareil de fonctionner en toute sécurité et de manière fluide.
- ✓ **Protection contre l'hameçonnage**
 - Les applis Téléphone de Google et Messages par Google permettent de détecter et de prévenir les attaques d'hameçonnage.
 - La navigation sécurisée de Google protège plus de 5 milliards d'appareils dans le monde.

Sécurité des applis

Un logiciel anti-malware prêt à l'emploi permet d'écartier les applications malveillantes, et des informations sur la sécurité des données obligent les développeurs à être transparents sur les applications téléchargées par les utilisateurs.

- ✓ **Google Play Store** : Des outils de détection alimentés par l'apprentissage automatique, ainsi que par des analystes humains, examinent toutes les applications avant qu'elles ne soient disponibles en téléchargement. La section Sécurité des données donne des informations sur le type de données collectées par l'application et sur l'usage qui en est fait.
- ✓ **Google Play Protect** : Analyse chaque jour plus de 125 milliards d'applications et notifie, supprime ou désactive les applications présentant des risques de sécurité.
- ✓ **App Defense Alliance (ADA)** : Google a collaboré avec les principaux partenaires qui oeuvrent à la détection des menaces contre les appareils mobiles pour fonder l'App Defense Alliance (ADA). Cet organisme a pour mission de protéger les utilisateurs Android contre les menaces potentiellement dangereuses (Potentially Harmful Applications, PHA) grâce au partage d'informations et à la coordination de processus de détection.

Sécurité de l'loT

Les labels de sécurité de l'loT indiquent clairement les pratiques en matière de confidentialité et de sécurité d'un appareil, comme le type de données collectées.

- ✓ Nous défendons un système basé sur cinq principes fondamentaux pour les **schémas de labellisation de la sécurité de l'loT** : labellisation « en direct », schémas d'évaluation, niveaux minimums de sécurité de référence couplés à une certaine flexibilité, transparence à grande échelle et incitations à l'adoption.
- ✓ Nous travaillons avec la Connectivity Standards Alliance (CSA) et la GSM Alliance (GSMA) pour normaliser un programme de certification à l'échelle du secteur qui réponde aux exigences réglementaires actuelles et futures.

Nos principes

Chez Google, nous appliquons 3 principes fondamentaux pour la sécurité et la transparence de nos appareils connectés :

Protection en profondeur : nous utilisons une architecture à plusieurs niveaux de sécurité qui fonctionnent ensemble pour une protection solide, fluide et efficace.

Ouverture et transparence : la transparence est au cœur de notre philosophie. Nous sommes persuadés qu'un écosystème open source peut se révéler **plus sécurisé** qu'un écosystème fermé, c'est pourquoi nous tenons informés les utilisateurs de notre plateforme et nous partageons nos connaissances pour renforcer nos systèmes de protection.

Le meilleur de Google et de notre écosystème : nous travaillons en partenariat avec des équipes spécialisées internes à Google et de toute l'industrie, pour protéger plusieurs milliards d'utilisateurs.

Applications

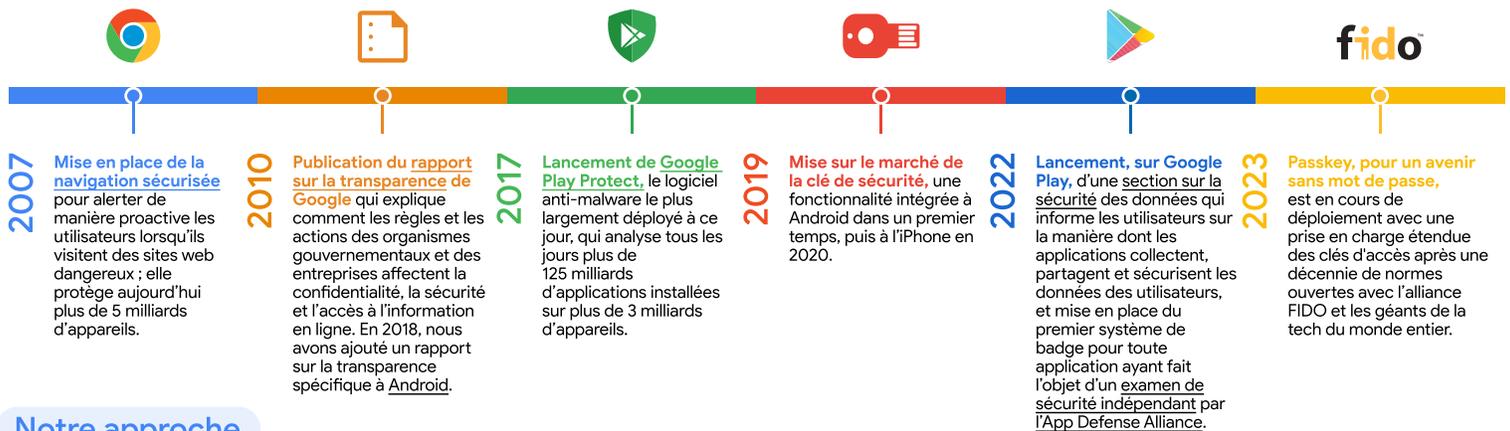
Labels de sécurité pour l'IoT : placer le consommateur en situation de contrôle

En l'absence de labels de sécurité pour l'IoT, les fabricants d'appareils ne sont pas tenus de respecter des normes mondiales. De leur côté, les utilisateurs n'ont aucune visibilité sur la manière dont leurs appareils protègent leurs données. Le secteur doit unir ses efforts pour faire progresser la sécurité de l'IoT et redonner le contrôle aux consommateurs. Nous travaillons à la mise en place d'un système de labellisation de la sécurité de l'IoT via nos processus et nos partenariats.

Nous investissons tout d'abord dans la [recherche en cybersécurité](#) dans le but d'identifier les éventuelles vulnérabilités (Google Nest participe au [programme de récompense des vulnérabilités](#) de Google et offre des récompenses aux chercheurs en cybersécurité qui, en dehors de Google, traquent et trouvent des vulnérabilités). Tous nos appareils développés en 2019 et au-delà utilisent [Verified Boot](#) pour garantir que le bon logiciel fonctionne et que l'accès est protégé. C'est notamment le cas de nos [appareils Google Nest](#) qui sont validés sur la base de normes de sécurité tierces reconnues par le secteur, telles que celles produites par les organismes de normalisation ETSI et ISO.

Ces normes, ainsi que notre cycle de vie sécurisé pour le développement des logiciels (SDLC), réduisent la probabilité que les consommateurs soient exposés à de mauvaises pratiques en matière de sécurité et ouvrent la voie à un internet ouvert et plus sûr.

Nos investissements dans le secteur et étapes clés



Notre approche

Mobilisés pour un monde numérique ouvert et sécurisé

Avec l'augmentation du nombre de données sur un plus grand nombre d'appareils connectés à différents réseaux, les questions de sécurité se font de plus en plus pressantes. Nous contribuons à faire progresser l'avenir de la sécurité des appareils connectés grâce au développement de nos produits, à nos critères de transparence et à nos partenariats avec les entreprises du secteur.

La sécurisation par défaut de tous nos produits est au centre de notre stratégie. La navigation sécurisée, Google Play Protect et les clés de sécurité intégrées protègent les appareils mobiles et les applications et assurent le niveau de sécurité le plus élevé de nos produits.

En faisant preuve d'ouverture et de transparence sur la façon dont nous traitons les failles et en partageant nos connaissances en matière de sécurité des appareils connectés, nous contribuons à la démocratisation de la sécurité opérationnelle. Nous sommes persuadés qu'un écosystème open source peut se révéler plus sûr qu'un écosystème fermé grâce à notre approche multicouche de la sécurité.

En collaborant avec des organismes tels que la CSA, l'ADA et la GSMA, nous mettons tout en œuvre pour faire progresser l'état de l'art en matière de cybersécurité, tout en ouvrant la voie à un internet et à un avenir plus sûrs pour tous.



Nous nous engageons à relever le niveau de sécurité des appareils connectés et à mettre en place des normes garantissant un environnement en ligne plus sûr pour tous et partout. Pour en savoir plus sur les progrès de Google en matière de sécurité des appareils connectés : g.co/connecteddevicesafety