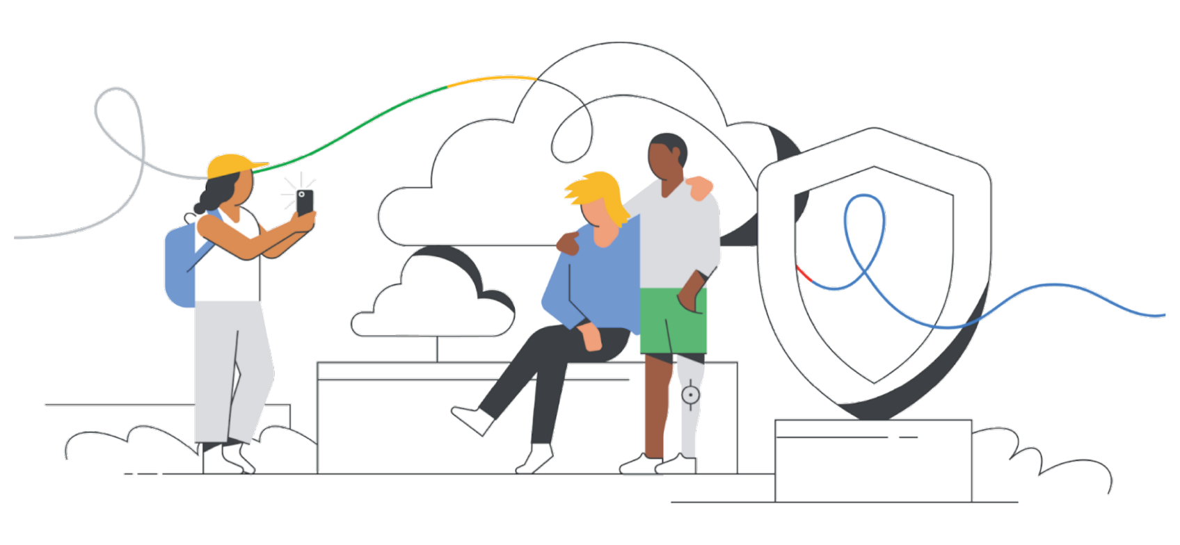
Notre expérience de la cybersécurité au fil des années

Sécurité renforcée avec Google

Nous assurons la sécurité en ligne des personnes mieux que quiconque dans le monde

Face à la montée en flèche des cyberattaques soutenues par certains États et autres acteurs malveillants en ligne, nous pensons que la sûreté de nos produits et services devient tout aussi importante que leur utilité.

Chez Google, nous sommes plus que jamais mobilisés pour protéger les personnes, les entreprises et les gouvernements en partageant notre expertise, en donnant à la société les moyens de faire face aux cyberrisques en constante évolution et nous efforçant de faire progresser les pratiques de pointe en matière de cybersécurité afin de construire un monde plus sûr pour tous.



Une série ininterrompue d'innovations

Depuis le lancement de Gmail en 2004 jusqu'à l'introduction de Protected Computing en 2022, Google a toujours démontré sa grande maîtrise des technologies de la cybersécurité. Nous n'avons pas cessé d'innover en matière de produits, de plateformes et de partenariats pour éliminer des catégories entières de menaces et créer un avenir plus sûr pour les personnes, les entreprises et les sociétés. Nos réalisations :

- ✓ Développement de plateformes et produits sûrs
- ✓ Formation d'équipes de sécurité agiles
- ✓ Création de programmes et de partenariats
- ✓ Financement essentiel pour l'innovation et la formation du personnel

Au fur et à mesure de l'évolution des besoins des individus et d'Internet, nous restons à l'avant-garde des nouvelles technologies afin d'atténuer les effets de la nature toujours changeante des cybermenaces et de faire en sorte que chaque jour soit plus sûr avec Google.

2004
Filtre antipourriel Gmail

Nous avons été l'un des premiers à mettre en place des filtres antipourriel basés sur l'IA pour les courriels.

99,9 % des messages dangereux et suspects sont bloqués par Gmail

2007
Navigation sécurisée

Nous contribuons de manière proactive à la protection d'appareils du monde entier en alertant les utilisateurs lorsqu'ils visitent des sites Web dangereux. En 2020, nous avons fait évoluer cette protection avec la navigation sécurisée améliorée.

5 milliards d'appareils protégés par la navigation sécurisée

2009
reCAPTCHA

Nous avons trouvé une riposte aux fraudes réalisées à l'aide de robots de recherche pour mettre un terme à l'utilisation d'identifiants usurpés et à la prise de contrôle de comptes, et pour prévenir les activités abusives des maliciels et des faux utilisateurs.

5 millions de sites Web protégés

2008
Gestionnaire de mots de passe Google

Le gestionnaire de mot de passe a rendu la connexion plus facile et plus sécurisée, en supprimant le besoin de retenir ou de saisir son mot de passe. Il est désormais utilisé pour 50 % de toutes les connexions à partir de Chrome, toutes plateformes confondues.

1 milliard de mots de passe vérifiés quotidiennement suite à des vols

2010
À vérification systématique

Après avoir survécu à l'opération Aurora, une série coordonnée de cyberattaques, nous avons radicalement changé notre approche pour bâtir une architecture sécurisée par défaut à vérification systématique (Zero Trust). Cette architecture permet de réduire les vecteurs d'attaque, limite les pertes de données tout en offrant un meilleur contrôle sur les systèmes dont dépendent les utilisateurs. Nous soutenons les efforts de la Maison Blanche qui a encouragé le déploiement par le gouvernement fédéral du modèle de sécurité à vérification systématique que nous avons également intégré dans BeyondCorp Enterprise, pour qu'il soit utilisé par toutes les entreprises qui le souhaitent.

2010
Threat Analysis Group (TAG)

Après l'opération Aurora, nous avons mis sur pied une équipe spécialisée comptant des experts chargés de détecter, d'analyser et de contrer les cybermenaces les plus graves soutenues par les gouvernements. Le TAG a attribué Wanna Cry, la plus grande attaque de logiciel de rançon de l'histoire, à la Corée du Nord, et a récemment partagé des exemples d'écosystèmes de piratage informatique en Inde, en Russie et aux Émirats arabes unis.

2010
Programme Bug Hunters de Google

Notre programme de récompense des vulnérabilités attire des étudiants, des juristes, des professionnels des TI et des passionnés qui traquent les bogues cachés dans les produits Google, en échange de contreparties financières. Si leurs motivations sont variées, leur mission est la même : trouver des vulnérabilités non découvertes afin de garantir la sécurité et la sûreté des services en ligne.

Des millions de dollars sous forme de récompenses depuis 2010

2010
L'équipe rouge

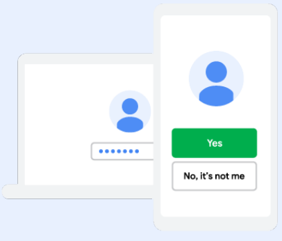
La mission de ses membres consiste à se mettre dans l'état d'esprit d'un adversaire pour renforcer nos défenses et repérer des failles. Basés dans le monde entier, ils exercent une veille des menaces actuelles, améliorent les contrôles de sécurité, détectent/préviennent les attaques et éliminent des catégories entières de vulnérabilités en mettant en place des cadres nouveaux et améliorés.

2013
Le projet Shield

Le projet Shield a contribué à protéger des organismes de presse, des associations de défense des droits de la personne, des sites électoraux, des organisations politiques et des campagnes contre les attaques par déni de service distribué (DDoS) dans plus de 100 pays en identifiant les menaces et en permettant à la communauté de la sécurité et aux forces de l'ordre d'y répondre.

Plus de 150 sites Internet actuellement protégés en Ukraine

2011
La vérification en 2 étapes



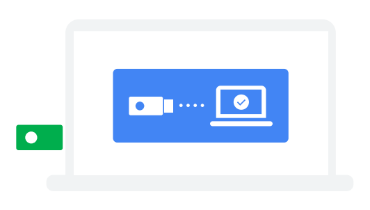
Nous avons été parmi les premiers à proposer la vérification en deux étapes (2SV) par défaut, et les premiers à l'activer automatiquement auprès de plus de 150 millions de personnes en 2021, pour une connexion simple et sécurisée. Votre compte est protégé, même en cas de vol de votre mot de passe.

Réduction de 50 % des comptes compromis depuis l'activation de la 2SV

2014
Project Zero

Il s'agit d'un groupe de travail spécialisé qui traque les vulnérabilités aux attaques de jour zéro sur Internet, dans les logiciels, le matériel, les produits Google et au-delà, afin de garantir un Internet sûr et ouvert. Les ingénieurs de ce groupe ont été les premiers à identifier les failles « Meltdown » et « Spectre », ce qui a permis aux développeurs de remédier rapidement aux vulnérabilités des CPU et d'appliquer des mesures d'atténuation tout au long de la chaîne d'approvisionnement logicielle.

2017
Programme de protection avancée



Il offre une sécurité renforcée, intégrant une clé de sécurité, aux utilisateurs qui possèdent des informations hautement visibles et sensibles, tels que les journalistes et les représentants des gouvernements.

+300 campagnes fédérales protégées

2018
Clé de sécurité Titan

Nous avons conçu la clé de sécurité Titan pour les utilisateurs à la recherche d'une solution Google de bout en bout. Conforme aux standards FIDO, cette clé peut être utilisée avec toute une gamme d'applis et de services, et pas seulement avec Google.

2019
Authentification sans mot de passe

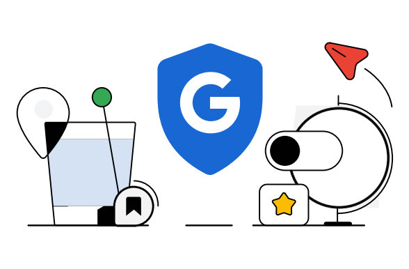
Extension de la prise en charge de FIDO par Android pour permettre aux utilisateurs de se connecter de manière transparente à des sites Web avec un NIP ou via le capteur biométrique, sans mot de passe.

2017
Google Play Protect

Google Play Protect est le service de protection contre les menaces sur les appareils mobiles le plus déployé au monde. Il s'adapte et s'améliore en permanence grâce à l'apprentissage automatique de Google. Google Play Protect analyse automatiquement les applis à la recherche de maliciels et chiffre les paiements effectués par les utilisateurs de téléphones Android.

Plus de 100 milliards d'applis analysées chaque jour pour détecter des maliciels

150 millions de paiements cryptés chaque jour



2019
Chronicle

Conçu comme une couche spécialisée de notre infrastructure principale, Chronicle est un service infonuagique qui permet aux entreprises de conserver, d'analyser et de rechercher des quantités importantes de données de sécurité et de réseau.

2021
Investir pour renforcer la cybersécurité

Nous sommes mobilisés pour renforcer la cybersécurité, élargir la portée de nos programmes à vérification systématique, sécuriser la chaîne d'approvisionnement logicielle et améliorer la sécurité des logiciels ouverts. Dans le cadre du programme Certificats de carrière Google, nous nous sommes engagés à former 100 000 Américains dans des domaines tels que le soutien des TI et l'analyse de données.

Engagement de 10 milliards de dollars pour des initiatives liées à la cybersécurité

2021
Informatique confidentielle

Pour traiter les questions essentielles de sécurité, de sûreté et de confidentialité, nous avons mis au point l'informatique confidentielle de Google Cloud, une technologie révolutionnaire qui permet de chiffrer les données pendant leur traitement et de les sécuriser tout au long de leur cycle de vie, y compris lorsqu'elles sont au repos ou en transit. Désormais, même les données les plus sensibles peuvent être migrées en toute confiance vers le nuage.

2021
Google Open Source Security Team (GOSST)

Le GOSST a été créé pour améliorer la sécurité des logiciels de code ouvert utilisés à travers le monde. Nous nous sommes associés à l'Open Source Security Foundation (OpenSSF) pour développer et publier le Supply-chain Levels for Software Artifacts (SLSA), un cadre de sécurisation de la chaîne d'approvisionnement logicielle, et assurer la sécurité à long terme de l'ensemble de l'écosystème des logiciels.

10 millions de dollars pour la correction de vulnérabilités dans les opérations de sécurité d'entreprises tierces

2022
Normalisation de la cryptographie post-quantique

Résolument tournés vers l'avenir, nous continuons à développer des systèmes cryptographiques de nouvelle génération qui empêchent de casser les systèmes cryptographiques à clé publique et de compromettre les communications numériques. Le National Institute of Standards and Technology (NIST) a procédé à la sélection de candidats à la normalisation avec la participation de Google (SPHINCS+).

2022
Protected Computing

Nous avons annoncé Protected Computing, une série de technologies qui transforme la manière, le moment et l'endroit où les données sont traitées afin de protéger techniquement la vie privée et la sécurité de l'utilisateur. Pour obtenir ce résultat, nous minimisons l'empreinte des données, en les dépersonnalisant et en limitant l'accès aux données sensibles. Cela signifie qu'Android peut suggérer la phrase suivante, tout en gardant la conversation complètement privée.

2023
La clé d'accès : l'avenir sans mots de passe

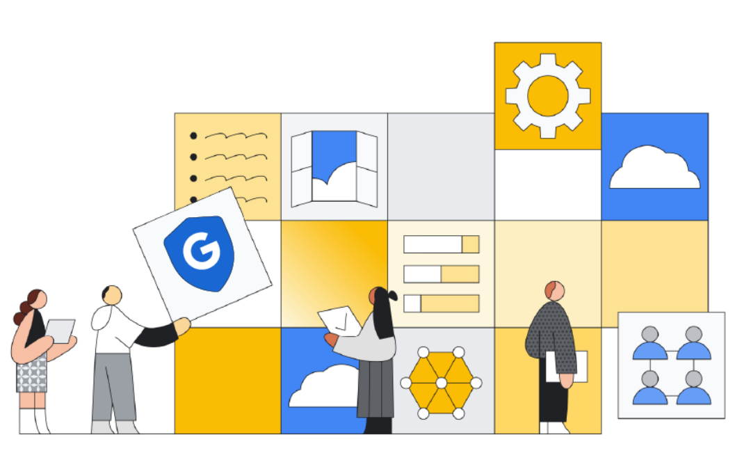
Depuis plus de dix ans, nous préparons un avenir sans mot de passe. En 2013, nous avons rejoint l'alliance FIDO dans le but de promouvoir des normes ouvertes pour un monde sans mot de passe. Avec la prise en charge des normes FIDO par Android et Chrome grâce à la technologie des clés d'accès en 2023, nous disposons désormais de la plateforme pour un véritable avenir sans mot de passe.

2022
Mandiant et Google Cloud

Fort de son expertise en cybersécurité acquise auprès des plus grandes entreprises mondiales, Mandiant fournit des informations approfondies sur les menaces en temps réel. Cette expertise, combinée aux offres de sécurité natives en nuage de Google Cloud, nous permet de protéger les entreprises et les organismes du secteur public tout au long du cycle de vie de la sécurité.

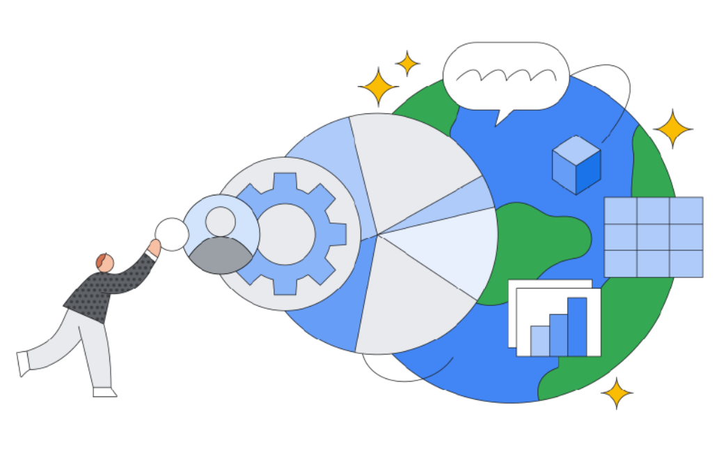
À une époque où les technologies ne cessent d'évoluer, la confiance dans les technologies est essentielle pour libérer le véritable potentiel de la société.

Tout en mettant en pratique nos connaissances dans le domaine de la sécurité, nous continuerons à collaborer avec les personnes, les entreprises et les gouvernements pour assurer leur sécurité et faire entrer la cybersécurité dans une nouvelle ère.



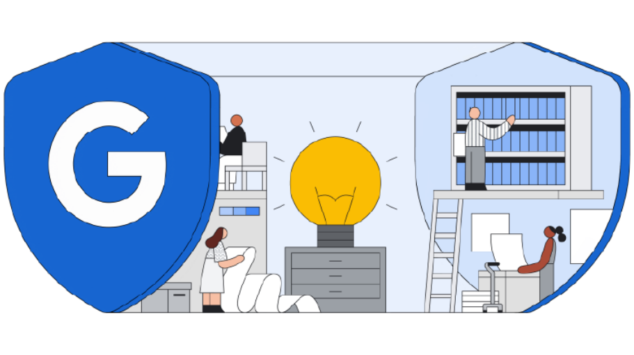
Protéger les personnes, les entreprises et les gouvernements

La sécurité est au centre de notre stratégie produit. C'est pourquoi tous nos produits sont dotés de protections intégrées qui les rendent sécurisés par défaut.



Donner à la société les moyens de faire face à l'évolution des risques en matière de cybersécurité

Nous mettons la société en position d'exploiter tout le potentiel des codes ouverts, et nous partageons notre savoir et notre expertise de manière transparente avec le secteur pour rendre les écosystèmes plus sûrs.



Faire émerger les futures technologies

Nous avons pour objectif de protéger la société contre la nouvelle génération de cybermenaces. Forts de notre expertise en matière d'IA, nous mettons au point les architectures du futur destinées à repousser les frontières de l'innovation.

Vous êtes toujours plus en sécurité avec Google

Visitez g.co/safety/cyber