Google

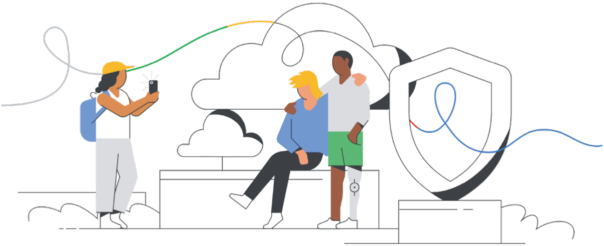
Notre expérience de la cybersécurité acquise au fil des années

En sécurité avec Google

Google travaille chaque jour à rendre Internet plus sûr pour tous

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.



Une série ininterrompue d'innovations

Du lancement de Gmail en 2004 jusqu'à l'introduction du Protected Computing en 2022, Google a toujours été pionnier en matière de technologies de 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, notamment grâce :

- ✓ Au développement de produits et de plateformes sécurisés
- ✓ À la formation d'équipes de sécurité agiles

- ✓ À la création de programmes et de partenariats
- ✓ Au financement de l'innovation et de la formation des professionnels

Alors qu'internet et que les besoins des individus évoluent, nous restons à l'avant-garde des nouvelles technologies afin d'atténuer les effets de cybermenaces en constante évolution, pour améliorer la sécurité de tous jour après jour.

2004
Filtre antispam Gmail

Nous avons été l'une des premières entreprises à mettre en place des filtres antispam basés sur l'IA pour les e-mails.

⊘ **99,9 %** des emails dangereux et suspects sont bloqués ⚠ par Gmail

2007
Navigation sécurisée

Nous contribuons de manière proactive à la protection des appareils dans le 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

2008
Gestionnaire de mots de passe Google

Le gestionnaire de mots de passe a rendu les connexions plus simples et plus sécurisées, 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 pour s'assurer qu'ils ne sont pas concernés par une violation de données

2009
reCAPTCHA

Nous avons fait l'acquisition de cette solution de gestion des fraudes et des bots pour mettre un terme à l'utilisation d'identifiants usurpés et au piratage de comptes, et empêcher les activités abusives des logiciels malveillants et des faux utilisateurs.

⚠ **5 millions** de sites web protégés

2010
Zéro confiance

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, connue aujourd'hui sous le nom « 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 Zero Trust 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 d'experts spécialisés, chargéee de détecter, d'analyser et de contrer les cybermenaces les plus graves et celles soutenues par des gouvernements. Le TAG a attribué Wanna Cry, la plus grande attaque de ransomware 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 de l'informatique et des passionnés qui traquent les bugs 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 des services en ligne.

Plusieurs millions de dollars sous forme de récompenses depuis 2010

2010
The Red Team

Sa mission est de se mettre dans l'état d'esprit d'un adversaire pour renforcer nos défenses et repérer des failles. Basés dans le monde entier, les membres de l'équipe 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 de nouveaux et meilleurs systèmes.

2013

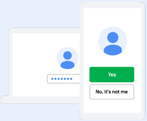
Project Shield

Project Shield a contribué à protéger des organismes de presse, des associations de défense des droits humains, des sites électoraux, des organisations politiques et des équipes de campagne 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 premières entreprises 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

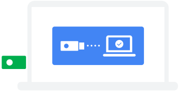
2014

Project Zero

Il s'agit d'un groupe de travail spécialisé qui traque les vulnérabilités de type « zero day » sur internet, dans les logiciels, le matériel informatique, 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 « Specter », 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 (APP)



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.

Plus de 300 campagnes fédérales protégés

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 au machine learning de Google. Google Play Protect analyse automatiquement les applications à la recherche de logiciels malveillants et chiffre les paiements effectués par les utilisateurs de téléphones Android.

Plus de 100 milliards d'applications analysées chaque jour pour détecter des logiciels malveillants

150 millions de paiments cryptés 🔒 chaque jour

2018

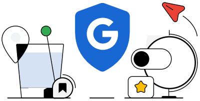
Clé de sécurité Titan

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

2019

Ré-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 PIN ou via le capteur biométrique, sans mot de passe.



2019

Chronicle

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

2021

Investir pour renforcer la cybersecurité

Nous sommes mobilisés pour renforcer la cybersécurité, élargir la portée de nos programmes zero trust, sécuriser la chaîne d'approvisionnement logicielle et améliorer la sécurité des logiciels open source. Dans le cadre du programme Google Career Certificate, nous nous sommes engagés à former 100 000 Américains dans des domaines tels que l'assistance informatique et l'analyse de données.

Investissement de **10 milliards de $** pour des initiatives liées à la cybersecurité

2021

Confidential Computing

Pour traiter les questions critiques de sécurité, de sûreté et de confidentialité, nous avons mis au point le Google Cloud Confidential Computing, 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 cloud.

2021

Google Open Source Security Team (GOSST)

Le GOSST (équipe de sécurité de l'open source) a été créé pour améliorer la sécurité des logiciels open source 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.

100 millions de $ 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 de 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 standardisation avec la participation de Google (SPHINCS+).

2022

Protected Computing

Nous avons annoncé le lancement de Protected Computing, une série de technologies qui transforment 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 entièrement privée.

2023

Passkey : l'avenir sans mot 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 (passkey) en 2023, nous disposons désormais de la plateforme permettant véritablement un avenir sans mot de passe.

2022

Mandiant et Google Cloud

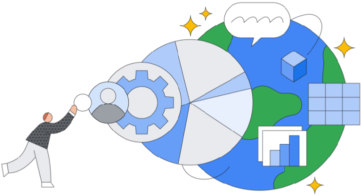
Fort de son expertise en cybersécurité acquise auprès des plus grandes entreprises mondiales, Mandiant fournit des informations approfondies sur les menaces en temps réel. Cette expertise, combinée aux offres de sécurité de Google Cloud intégrées sur le cloud, nous permet de protéger les entreprises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

À une époque où la technologie ne cesse d'évoluer, la confiance 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 de collaborer avec les personnes, les entreprises et les gouvernements pour assurer leur sécurité et faire entrer la cybersécurité dans une nouvelle ère.

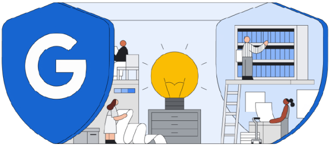
Protéger les personnes, les entreprises et les gouvernements

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 fournissons à la société les moyens d’exploiter tout le potentiel de l’open source, et nous partageons nos connaissances 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.

En sécurité chaque jour avec Google

Visiter g.co/safety/cyber

Google