Google

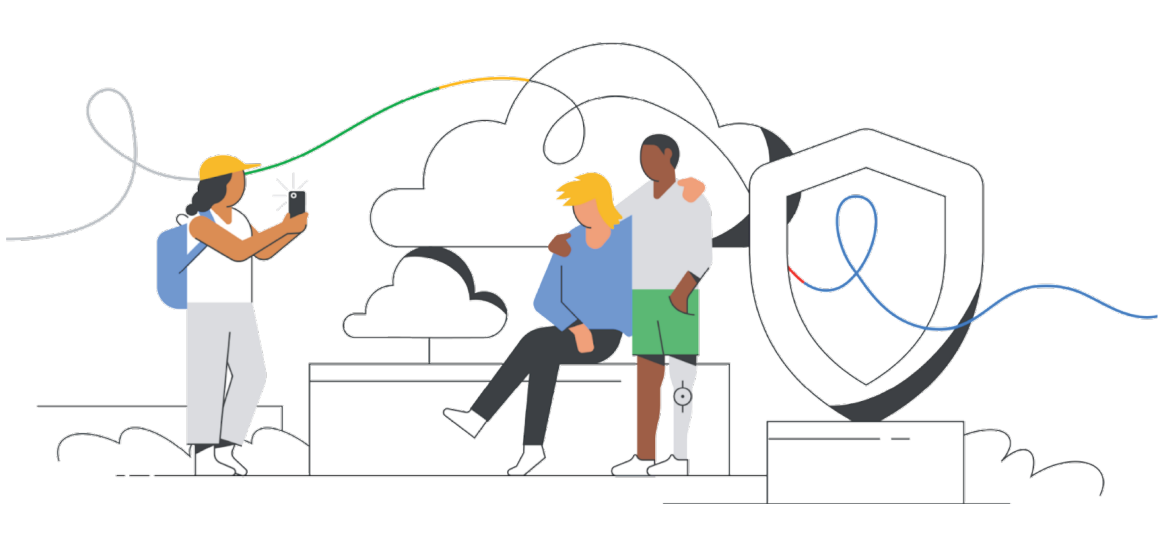
Călătoria noastră în domeniul securității cibernetice

Mai în siguranță cu Google

Menținem mai mulți oameni în siguranță online decât oricine altcineva în lume

Dată fiind creșterea puternică a atacurilor cibernetice sponsorizate de anumite state și a actorilor rău-intenționați online, credem că produsele și serviciile noastre sunt utile doar în măsura în care sunt securizate.

La Google, suntem mai concentrați ca niciodată să protejăm oamenii, organizațiile și autoritățile guvernamentale prin împărtășirea experienței noastre, să ajutăm societatea să facă față riscurilor cibernetice din ce în ce mai mari și să lucrăm permanent pentru a dezvolta o securitate cibernetică de vârf, în vederea construirii unei lumi mai sigure pentru toți oamenii.



Inovația continuă, de-a lungul timpului

De la lansarea Gmail, în 2004, și până la introducerea proceselor informatice protejate, în 2022, Google a jucat un rol de pionier în tehnologia securității cibernetice și a inovat continuu produsele, platformele și parteneriatele pentru a elimina clase întregi de amenințări, în vederea creării unui viitor mai sigur pentru oameni, organizații și societăți, prin:

- Dezvoltarea produselor și platformelor securizate
- Construirea unor echipe de securitate agile
- Încurajarea programelor și parteneriatelor
- Furnizarea finanțării esențiale pentru inovație și instruirea forței de muncă

Pe măsură ce nevoile oamenilor și internetul evoluează, continuăm să fim în avangarda noilor tehnologii, pentru a diminua amenințările cibernetice în continuă schimbare și a garanta că fiecare zi este mai sigură cu Google.

2004
Protecția Gmail împotriva spam

Am fost printre primii care au introdus protecții e-mail controlate de AI încorporate.

99,9% dintre e-mailurile periculoase și suspecte sunt blocate de Gmail

2007
Navigarea sigură

Ajutăm la protejarea proactivă a dispozitivelor din întreaga lume prin alertarea utilizatorilor când vizitează site-uri web periculoase, evoluând aceste protecții online spre Navigarea sigură îmbunătățită, în 2020.

5 miliarde de dispozitive protejate de Navigarea sigură

2008
Managerul de parole Google

Introducerea managerului de parole a făcut conectarea mai ușoară și mai sigură, fără nevoia de a reține sau tasta parola, fiind utilizat acum pentru 50% dintre conectările din Chrome, pe toate platformele.

1 miliard de parole verificate zilnic pentru eventuale breșe

2009
reCAPTCHA

Am achiziționat soluția de control al fraudelor și boților pentru a opri încărcarea datelor de autentificare și preluările conturilor și pentru a preveni activitățile abuzive ale software-ului rău-intenționat/utilizatorilor falși.

5 milioane de site-uri web protejate

2010
Încredere zero

După supraviețuirea în fața Operațiunii Aurora, o serie coordonată de atacuri cibernetice, ne-am revoluționat abordarea arhitecturii de securitate implicită, cunoscută acum ca „Încredere zero”. Aceasta asigură mai puțini vectori de atac, mai puține oportunități de a pierde date și mai mult control asupra sistemelor pe care se bazează utilizatorii. Susținem eforturile Casei Albe de a desfășura modelul Încredere zero la nivelul tuturor autorităților guvernamentale federale și de a-l include și în BeyondCorp Enterprise, pentru ca orice întreprindere să poată beneficia de el.

2010
Grupul de analiză a amenințărilor - Threat Analysis Group (TAG)

După Operațiunea Aurora, am alcătuit o echipă specializată de experți responsabilă pentru detectarea, analizarea și eliminarea amenințărilor cibernetice infracționale grave și susținute de guverne. TAG a identificat Wanna Cry, cel mai mare atac de ransomware din istorie, ca provenind din Coreea de Nord, și, recent, a făcut publice exemple de ecosisteme de hacking pe bază de contract din India, Rusia și Emiratele Arabe Unite.

2010
Echipa roșie

A fost lansată pentru a simula modul de gândire al adversarilor și a ataca Google, pentru a ajuta la întărirea securității și a identifica lipsurile. Membrii acestei echipe lucrează la nivel global pentru a ține pasul cu amenințările actuale, a îmbunătăți controalele de securitate, a realiza detectarea/prevenirea atacurilor și a elimina clase întregi de vulnerabilități prin trasarea unor cadre de lucru noi și mai eficiente.

2010
Vânătorii de erori Google

Programul nostru de recompense pentru descoperirea vulnerabilităților atrage liceeni, avocați, profesioniști din domeniul IT și pasionați de vânătoarea de erori în produsele Google, pe baza premiilor în bani. Motivele acestora sunt diferite, dar misiunea este aceeași: să găsească vulnerabilități nedescoperite, pentru a menține servicii online sigure și securizate.

Milioane de dolari plătite ca recompense, începând din 2010

2011
Verificarea în 2 pași

Suntem printre primii care au oferit implicit verificarea în 2 pași (2SV) și primii care au activat automat 2SV pentru peste 150 de milioane de oameni, în 2021, oferind o modalitate sigură și ușoară de conectare. Chiar dacă ți se fură parola, contul tău este protejat.

50% reducere a numărului de conturi compromise de la introducerea 2SV

2013
Project Shield

Project Shield a ajutat la protejarea știrilor, a organizațiilor pentru apărarea drepturilor omului, a site-urilor electorale, a organizațiilor politice și a campaniilor împotriva atacurilor Distributed Denial of Service (DDoS) din peste 100 de țări împotriva atacurilor cibernetic prin identificarea amenințărilor și activarea răspunsurilor în comunitatea de securitate și de aplicare a legii.

150+ site-uri web protejate în prezent în Ucraina

2014
Project Zero

O echipă specializată, dedicată identificării atacurilor încă din ziua zero pe întregul internet - în software, hardware, produse Google și dincolo de acestea, pentru a asigura un internet sigur și deschis. Au fost primii care au descris în detaliu „Meltdown” și „Specter”, permițându-le dezvoltatorilor să rezolve rapid vulnerabilitățile de CPU și să aplice diminuări ale efectelor în întregul lanț de aprovizionare software.

2017
Programul de protecție avansată (APP)

Protecții de securitate suplimentare, inclusiv cheia de securitate, pentru utilizatorii cu înaltă vizibilitate și risc ridicat, cum sunt jurnaliștii și funcționarii guvernamentali.

300+ campanii federale protejate

2017
Google Play Protect

Serviciul de protecție împotriva amenințărilor pe dispozitive mobile implementat la scara cea mai largă din lume, adaptându-se și îmbunătățindu-se în permanență prin învățarea automată Google, Google Play Protect scanează automat aplicațiile pentru a identifica malware și criptează plățile utilizatorilor pe telefoanele Android.

100+ miliarde de aplicații scanate zilnic pentru malware

150 de milioane de plăți ale utilizatorilor criptate zilnic

2018
Cheia de securitate titan

Am creat Cheia de securitate titan pentru utilizatorii care doresc o soluție Google end-to-end. Cheile sunt conforme cu FIDO și pot fi utilizate oriunde, nu doar pe Google.

2019
Reautentificarea fără parolă

Am extins asistența noastră FIDO în Android, pentru ca utilizatorii să se poată conecta fără probleme la site-uri web doar cu un cod PIN sau date biometrice, fără să fie necesară o parolă.

2019
Chronicle

Construit ca un strat specializat pe lângă infrastructura noastră esențială, Chronicle a fost introdus pentru a oferi organizațiilor securitate în cloud, în vederea păstrării, analizării și căutării confidențiale a unor volume mari de date despre securitate și rețele.

2021
Investiție pentru dezvoltarea securității cibernetice

Suntem angajați să consolidăm securitatea cibernetică, să extindem programele de încredere zero, să ajutăm la securizarea lanțului de aprovizionare software și să îmbunătățim securitatea surselor deschise. Ne-am angajat să instruim peste 100.000 de americani în domenii precum Asistență IT și Analiza datelor, prin programul Certificat de carieră Google.

Angajament de 10 miliarde de dolari pentru inițiativele din domeniul securității cibernetice

2021
Echipa Google pentru securitatea surselor deschise (GOSST)

GOSST a fost creată pentru a îmbunătăți securitatea software-ului din surse deschise, pe care se bazează lumea. Am încheiat un parteneriat cu Fundația pentru securitatea surselor deschise - Open Source Security Foundation (OpenSSF), pentru a dezvolta și lansa nivelurile lanțului de aprovizionare pentru artefacte software - Supply-Chain Levels for Software Artifacts (SLSA), un cadru de lucru pentru a securiza lanțul de aprovizionare software și a permite securitatea pe termen lung pentru întregul ecosistem software.

Angajament de 100 de milioane de dolari pentru operațiunile de securitate a surselor deschise desfășurate de terți, pentru a remedia vulnerabilitățile

2021
Procese informatice confidențiale

Pentru securitate, siguranță și confidențialitate în domenii critice, am introdus Google Cloud Confidential Computing, o tehnologie de vârf care păstrează datele criptate pe parcursul prelucrării, permițând menținerea securității lor pe tot parcursul ciclului de viață, inclusiv în timpul păstrării sau atunci când sunt în tranzit. Acum, chiar și cele mai sensibile date pot fi migrate în cloud, în condiții de confidențialitate.

2022
Standardizarea criptografiei post-quantum

Axați pe viitor, continuăm dezvoltarea următoarei generații de sisteme criptografice care protejează împotriva spargerii sistemelor de criptare cu cheie publică și compromiterea comunicațiilor digitale. Institutul Național de Standarde și Tehnologie a selectat un document realizat cu implicarea Google (SPHINCS+) pentru standardizare.

2022
Procese informatice protejate

Am anunțat Procesele informatice protejate, un set de instrumente în continuă dezvoltare, care transformă modul, momentul și locul în care datele sunt prelucrate pentru a asigura confidențialitatea și siguranța utilizatorului, din punct de vedere tehnic. Facem acest lucru prin minimizarea amprentei datelor, de-identificarea datelor și restricționarea accesului la date sensibile. Aceasta înseamnă că Android poate sugera următoarea frază din text, păstrând în același timp confidențialitatea întregii conversații.

2022
Mandiant și Google Cloud

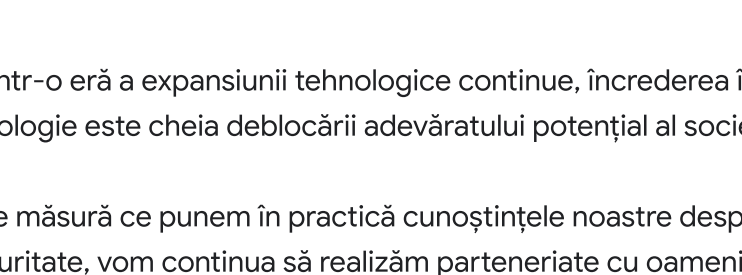
Mandiant oferă informații în timp real, aprofundate, despre amenințări, obținute în prima linie a securității cibernetice, cu ajutorul celor mai mari organizații din lume. Prin combinarea cu ofertele de securitate native în cloud ale Google Cloud, ajutăm întreprinderile și agențiile din sectorul public să rămână protejate pe parcursul întregului ciclu de securitate.

2023
Codul de acces: viitorul fără parole

Pregătim, de peste un deceniu, terenul pentru un viitor fără parole. Am intrat în Alianța FIDO, în 2013, pentru adoptarea unor standarde deschise, pentru o lume fără parole, și acum ne extindem sprijinul pentru standardele de conectare FIDO la Android și Chrome prin tehnologia codurilor de acces, iar în 2023 vom avea, în sfârșit, platforma pentru un viitor cu adevărat fără parole.

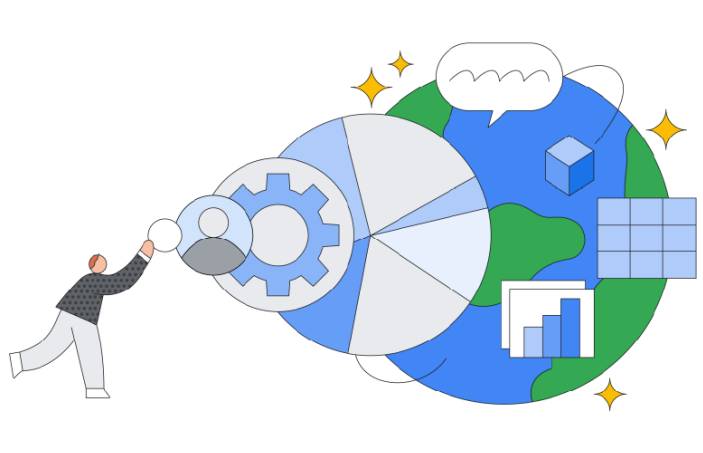
Într-o eră a expansiunii tehnologice continue, încrederea în tehnologie este cheia deblocării adevăratului potențial al societății.

Pe măsură ce punem în practică cunoștințele noastre despre securitate, vom continua să realizăm parteneriate cu oamenii, cu firmele și cu autoritățile guvernamentale pentru a le proteja siguranța și a da impulsul unei noi ere a securității cibernetice.



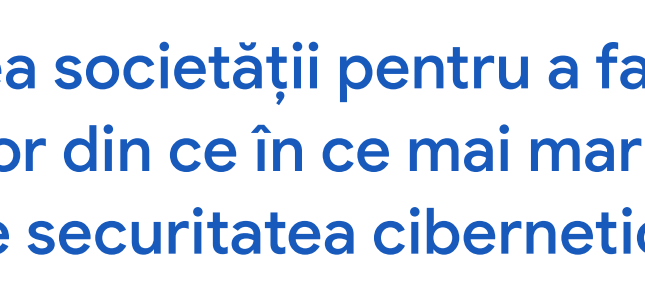
Protejarea oamenilor, a firmelor și a autorităților guvernamentale

Securitatea este piatra de temelie a strategiei noastre pentru produse. De aceea, toate produsele noastre au protecții încorporate, care le garantează siguranța în mod implicit.



Ajutarea societății pentru a face față riscurilor din ce în ce mai mari legate de securitatea cibernetică

Noi oferim societății posibilitatea de a debloca potențialul surselor deschise și transmitem cunoștințele și experiența noastră în mod transparent în interiorul industriei, pentru a menține ecosistemul mai sigur.



Avansarea tehnologiilor viitoare

Dorim să protejăm societățile de următoarea generație de amenințări cibernetice. Pornind de la experiența noastră în domeniul AI, proiectăm următorul val de arhitecturi pentru a împinge limitele inovației în domeniul securității.

În fiecare zi ești mai în siguranță cu Google

Vizitați g.co/safety/cyber

Google