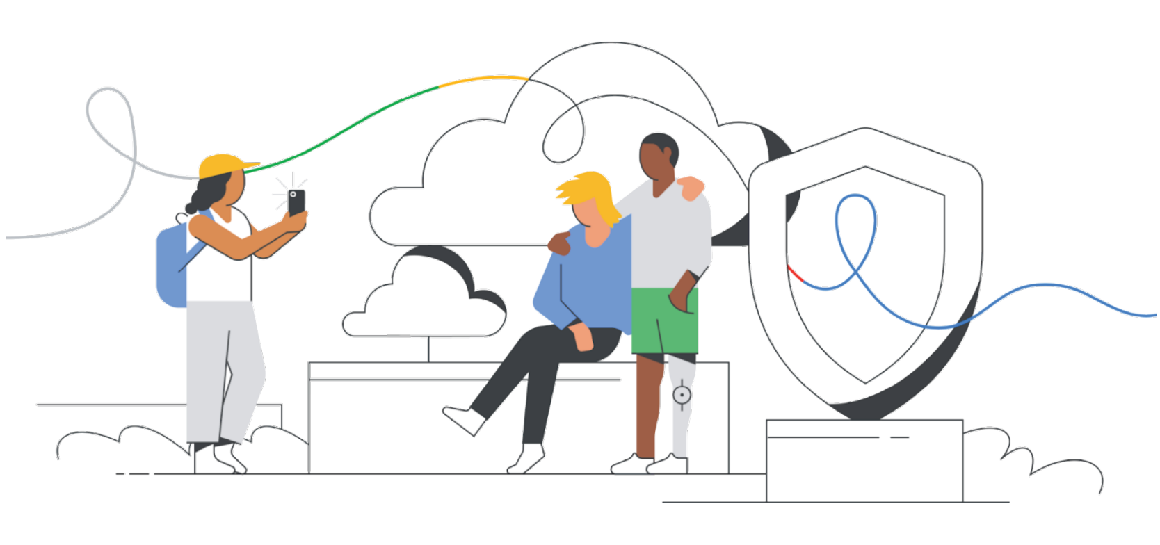
Vores cybersikkerhedsrejse gennem årene

Mere sikker med Google

Google arbejder hver dag på at gøre internettet mere sikkert for alle

Med den dramatiske stigning i statsfinansierede cyberangreb og ondsindede onlineaktører, mener vi, at vores produkter og tjenester kun er så nyttige, som de er sikre.

Hos Google er vi mere fokuserede end nogensinde på at beskytte mennesker, organisationer og regeringer ved at dele vores ekspertise, så vi kan gøre samfundet i stand til at håndtere cyberrisici, som hele tiden udvikles, og løbende arbejde for at forbedre det ypperste inden for cybersikkerhed for at skabe en sikrere verden for alle.



Løbende fornyelse gennem tiderne

Siden lanceringen af Gmail i 2004 til introduktionen af Beskyttet Computing i 2022, har Google været banebrydende inden for cybersikkerhedsteknologi og løbende innoveret på produkter, platforme og partnerskaber for at eliminere hele klasser af trusler for at skabe en sikrere fremtid for mennesker, organisationer og samfund ved at:

- ✓ Udvikle sikre produkter og platforme
- ✓ Opbygge smidige sikkerhedsteams
- ✓ Fremme programmer og partnerskaber
- ✓ Sørge for nødvendige midler til innovation og arbejdsstyrkeuddannelse

Efterhånden som både folks behov og internettet udvikler sig, fortsætter vi med at være på forkant med nye teknologier til at afbøde stadigt skiftende cybertrusler og sikre, at hver dag er sikrere med Google.

2004
Gmail spam-beskyttelse

Vi var blandt de første til at bygge AI-drevet e-mail-beskyttelse.

99.9 % af farlige og mistænkelige e-mails blokeres af Gmail

2007
Beskyttet browsing

Vi hjælper proaktivt med at beskytte enheder over hele verden ved at advare brugere, når de besøger farlige websteder, og videreudviklede disse onlinebeskyttelser til Forbedret Beskyttet browsing i 2020.

5 milliarder enheder beskyttet af Beskyttet browsing

2009
reCAPTCHA

Vi erhvervede svindel- og bothåndteringsløsningen for at stoppe udfyldning af legitimationsoplysninger og kontoovertagelser og for at forhindre misbrug fra ondsindet software/falske brugere.

5 millioner websteder forsvaret

2008
Google Adgangskodeadministrator

Introduktionen af Adgangskodeadministrator gjorde det nemmere og mere sikkert at logge ind uden at skulle huske eller indtaste din adgangskode og bruges nu til 50 % af alle logins i Chrome på tværs af platforme.

1 milliard adgangskoder kontrolleret dagligt for brud

2010
Zero Trust

Efter at have overlevet Operation Aurora, en koordineret serie af cyberangreb, revolutionerede vi vores tilgang til at bygge en sikker-by-default-arkitektur, nu kendt som "Zero Trust". Det sikrer færre angrebsspredere, færre muligheder for at miste data og mere kontrol over de systemer, brugerne er afhængige af. Vi støtter Det Hvide Hus' bestræbelser på at implementere Zero Trust-modellen på tværs af den føderale regering og har også lagt den ind i BeyondCorp Enterprise, så enhver virksomhed kan udnytte den.

2010
Threat Analysis Group (TAG)

Efter Operation Aurora oprettede vi et specialiseret team af eksperter, som er ansvarlige for at opdage, analysere og forstyrre statsstøttede og alvorlige kriminelle cybertrusler. TAG sporede Wanna Cry, det største ransomware-angreb i historien, til Nordkorea og delte for nylig eksempler på hack-for-hire-økosystemerne fra Indien, Rusland og De Forenede Arabiske Emirater.

2010
Google Bug Hunters

Vores Vulnerability Rewards-program tiltrækker med pengepræmier gymnasieelever, advokater, it-professionelle og hobbyfolk til at gå på jagt efter fejl i Google-produkter. Deres motiver varierer, men deres mission er den samme: At finde uopdagede sårbarheder for at holde onlinetjenester sikre.

Der er siden 2010 udbetalt belønninger for millioner af dollars

2010
The Red Team

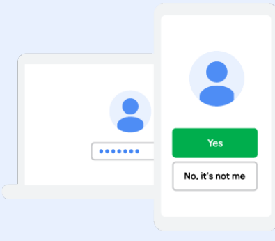
Lanceret for at påtage sig en kontradiktorisk tankegang og hacke Google for at hjælpe med at styrke vores forsvar og opdage huller. De arbejder over hele kloden for at holde trit med aktuelle trusler, forbedre sikkerhedskontrollen, udføre angrebssporing/-forebyggelse og eliminere hele klasser af sårbarheder ved at skabe nye og bedre rammer.

2013
Project Shield

Project Shield har hjulpet med at beskytte nyheder, menneskerettighedsorganisationer, valgsteder, politiske organisationer og kampagner fra Distributed Denial of Service (DDoS)-angreb i over 100 lande mod cyberangreb ved at identificere trusler og muliggøre reaktioner i sikkerhedssamfundet og retshåndhævelsen.

Over 150 websteder er i øjeblikket beskyttet i Ukraine

2011
Totrinsbekræftelse



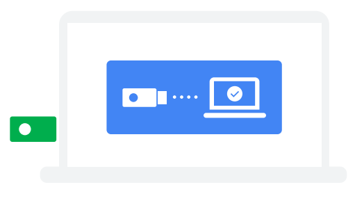
Vi var blandt de første til at tilbyde totrinsbekræftelse (2SV) som standard, og de første til automatisk at aktivere 2SV for over 150 millioner mennesker i 2021, hvilket gav en sikker og nem måde at logge på. Selvom din adgangskode bliver stjålet, er din konto beskyttet.

50 % fald i kompromitterede konti siden 2SV

2014
Project Zero

En specialiseret taskforce dedikeret til at jage 'nul dages-angribere' (zero day exploits) på tværs af internettet – i software, hardware, Google-produkter med mere for at sikre et sikkert og åbent internet. De var de første, der detaljeret beskrev "Meltdown" og "Specter", hvilket gjorde det muligt for udviklere hurtigt at adressere CPU-sårbarheder og anvende afbødninger på tværs af softwareforsyningskæden.

2017
Advanced Protection Program (APP)



Ekstra sikker beskyttelse, inklusive sikkerhedsnøgle, til brugere med høj synlighed og høj risiko, f.eks. journalister og embedsmænd.

Over 300 føderale kampagner beskyttet

2018
Titan Security Key

Vi lavede Titan-sikkerhedsnøglen til brugere, der ønsker en end-to-end Google-løsning. Nøglerne er FIDO-kompatible og kan også bruges andre steder, ikke kun med Google.

2019
Adgangskodefri gengodkendelse

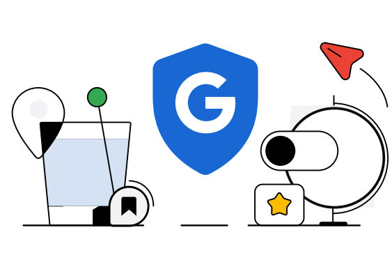
Udvidede vores FIDO-understøttelse i Android, så brugere problemfrit kunne logge på websteder med blot en PIN-kode eller biometrisk, uden behov for adgangskode.

2017
Google Play Protect

Den mest udbredte mobiltrusselsbeskyttelsestjeneste i verden, der konstant tilpasser sig og forbedres med Googles maskinlæring. Google Play Protect scanner automatisk apps for malware og krypterer brugerbetalinger på Android-telefoner.

Over 100 milliarder apps scannet for malware dagligt

150 millioner brugerbetalinger krypteret dagligt



2019
Chronicle

Chronicle blev bygget som et specialiseret lag oven på vores kerneinfrastruktur og blev introduceret for at levere cloud-baseret sikkerhed designet til virksomheder til privat at opbevare, analysere og søge i enorme mængder sikkerheds- og netværksdata.

2021
Investering for at fremme cybersikkerhed

Vi forpligter os til at styrke cybersikkerhed, udvide zero-trust-programmer, hjælpe med at sikre softwareforsyningskæden og forbedre open source-sikkerhed. Vi har garanteret at ville uddanne 100.000 amerikanere inden for områder som it-support og dataanalyse gennem Google Career Certificate-programmet.

10 milliarder USD som engagement i cybersikkerhedsinitiativer

2021
Confidential Computing

Af hensyn til kritisk sikkerhed, sikkerhed og privatliv introducerede vi Google Cloud Confidential Computing, en banebrydende teknologi, der holder data krypteret, mens de behandles, hvilket gør det muligt for dem at forblive sikre gennem hele deres livscyklus, inklusive i hvile eller under overførsel. Nu kan selv de mest følsomme data migreres sikkert til skyen.

2021
Google Open Source Security Team (GOSST)

GOSST blev oprettet for at forbedre sikkerheden for den open source-software, som verden er afhængig af. Vi indgik samarbejde med Open Source Security Foundation (OpenSSF) for at udvikle og frigive Supply-Chain Levels for Software Artifacts (SLSA), en ramme til at sikre softwareforsyningskæden og muliggøre langsigtet sikkerhed for hele softwareøkosystemet.

100 millioner USD er dedikeret til tredjeparts open source-sikkerhedsoperationer for at hjælpe med at løse sårbarheder

2022
Post-Quantum Cryptography Standardization

Vi fortsætter fremtidsfokuseret med at udvikle næste generations kryptografiske systemer, der sikrer mod brud på offentlige nøglekryptosystemer og kompromittering af digital kommunikation. National Institute of Standards and Technology valgte et bidrag med Googles involvering (SPHINCS+) til standardisering.

2022
Beskyttet Computing

Vi annoncerede Beskyttet Computing, et voksende værktøjssæt af teknologier, der forvandler, hvordan, hvornår og hvor data behandles for teknisk at sikre brugerens privatliv og sikkerhed. Det gør vi ved at minimere dataaftrykket, afidentificere data og begrænse adgangen til følsomme data. Det betyder, at Android kan foreslå den næste sætning i teksten, mens samtalen holdes helt privat.

2023
Passkey: Fremtiden uden adgangskoder

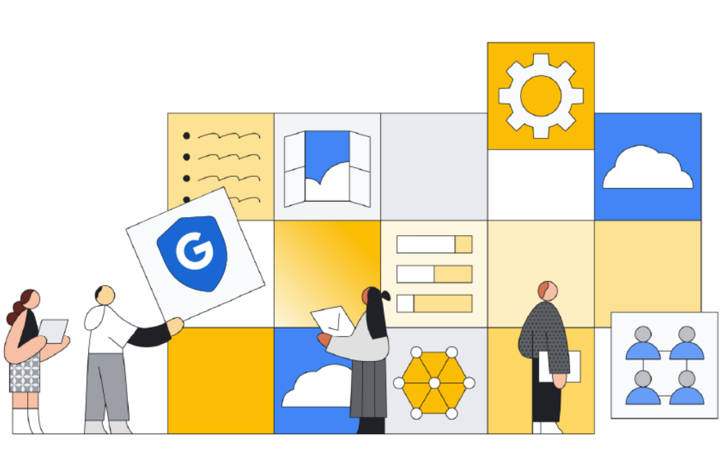
Vi har i over et årti forberedt en fremtid uden adgangskoder. Vi sluttede os til FIDO Alliance i 2013 for at fremme åbne standarder i en verden uden adgangskoder, og nu – ved i 2023 at udvide vores support til FIDO-loginstandarder til Android og Chrome gennem adgangsnøgleteknologi – får vi endelig platformen for en virkelig adgangskodeløs fremtid.

2022
Mandiant og Google Cloud

Mandiant tilbyder dybdegående trusselsintelligens, der er opnået på frontlinjen af cybersikkerhed i realtid med de største organisationer i verden. Kombineret med Google Clouds cloud-native sikkerhedstilbud hjælper vi virksomheder og offentlige myndigheder med at forblive beskyttet gennem hele sikkerhedslivscyklussen.

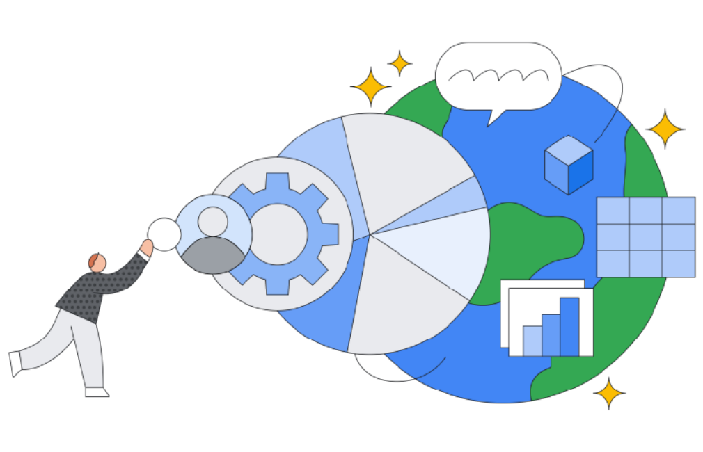
I en tid med stadigt voksende teknologisk rækkevidde er tillid til teknologi nøglen til at frigøre samfundets sande potentiale.

Efterhånden som vi omsætter vores sikkerhedsviden i praksis, vil vi fortsætte med at samarbejde med mennesker, virksomheder og regeringer for at beskytte deres sikkerhed og fremme en ny æra inden for cybersikkerhed.



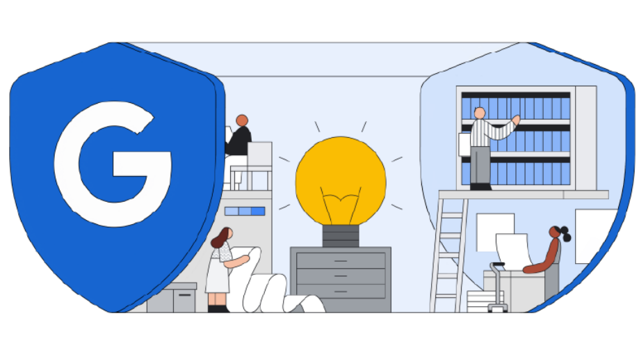
Beskyttelse af mennesker, virksomheder og regeringer

Sikkerhed er hjørnestenen i vores produktstrategi. Derfor har alle vores produkter indbygget beskyttelse, der som standard gør dem sikre.



Bemyndigelse af samfundet til at imødegå cybersikkerhedsrisici under udvikling

Vi giver samfund mulighed for at frigøre potentialet ved open source og deler vores viden og ekspertise gennemsigtigt med brancheindustrien for at holde økosystemerne sikrere. Fremme af fremtidens teknologier



Vi ønsker at beskytte samfund mod den næste generation af cybertrusler.

Med udgangspunkt i vores AI-ekspertise designer vi den næste bølge af arkitekturer for at skubbe grænserne for sikkerhedsinnovation.

Hver dag er du mere sikker med Google

Visit g.co/safety/cyber