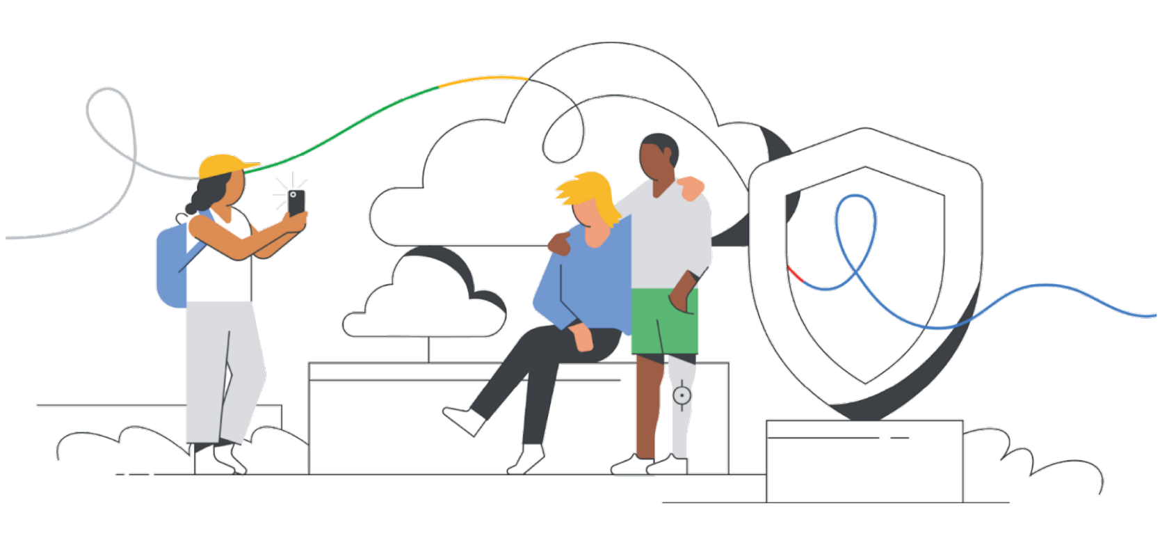
Onze cybersecurity-reis door de jaren heen

Veiliger met Google

Google werkt er iedere dag aan om het internet voor iedereen veiliger te maken

Met de dramatische toename van staatsgesponsorde hackersaanvallen en kwaadwillende individuen online, vinden we dat onze producten en diensten alleen nuttig zijn als ze echt veilig zijn.

Bij Google zijn we er meer dan ooit op gericht mensen, organisaties en overheden te beschermen door onze expertise te delen, de samenleving de middelen te geven om de steeds evoluerende digitale risico's aan te pakken en ons voortdurend in te zetten voor de bescherming van mensen en overheden, en voortdurend te werken aan verbetering van de stand van de techniek op het gebied van cybersecurity om zo een veiligere wereld voor iedereen te realiseren.



Voortdurende innovatie door de jaren heen

Vanaf de introductie van Gmail in 2004 tot en met de introductie van Veilig Computergebruik in 2022 heeft Google het voortouw genomen op het gebied van cybersecuritytechnologie en continu geïnnoveerd met producten, platforms en samenwerkingen om complete dreigingsklassen te elimineren en zo een veiligere toekomst te creëren voor mensen, organisaties en samenlevingen:

- Ontwikkeling van veilige producten en platforms
- Opbouw van flexibele beveiligingsteams
- Bevordering van programma's en samenwerkingsverbanden
- Verstrekking van essentiële financiering voor innovatie en opleiding van arbeidskrachten

De behoeften van mensen en het internet veranderen, en wij blijven vooroplopen met nieuwe technologieën om de steeds veranderende cyberbedreigingen te beperken, zodat elke dag veiliger wordt met Google.

2004
Gmail spambeveiliging

We waren een van de eersten die AI-gestuurde emailbeveiliging bouwden.

99,9% van de gevaarlijke en verdachte e-mail wordt geblokkeerd door Gmail

2007
Safe Browsing

We helpen proactief apparaten over de hele wereld te beschermen door gebruikers te waarschuwen wanneer ze gevaarlijke websites bezoeken. Deze online bescherming evolueert in 2020 naar Enhanced Safe browsing.

5 miljard apparaten beschermd door Safe Browsing

2008
Google Wachtwoordmanager

De introductie van Wachtwoordmanager maakte het aanmelden gemakkelijker en veiliger, zonder dat het nodig was je wachtwoord te onthouden of in te typen. Het wordt nu gebruikt voor 50% van alle aanmeldingen via Chrome op alle platforms.

1 miljard wachtwoorden dagelijks gecontroleerd op inbreuken

2009
reCAPTCHA

We hebben deze oplossing voor fraude- en botbeheer verworven om 'credential stuffing' en overname van accounts tegen te gaan en misbruik door schadelijke software/ nepgebruikers te voorkomen.

5 miljoen websites beschermd

2010
Zero Trust

Nadat we Operation Aurora, een gecoördineerde reeks cyberaanvallen, hadden overleefd, hebben we onze aanpak gerevolutioneerd om een 'secure-by-default' beveiligingsarchitectuur te bouwen die nu bekendstaat als 'Zero Trust'. Het zorgt voor minder aanvalsvectoren, minder mogelijkheden om gegevens te verliezen en geeft meer controle over de systemen waarvan gebruikers afhankelijk zijn. We ondersteunen de inspanningen van het Witte Huis om het Zero Trust-model te implementeren in de federale overheid. We hebben het ook geïntegreerd in BeyondCorp Enterprise zodat elke onderneming er gebruik van kan maken.

2010
Threat Analysis Group (TAG)

Na Operatie Aurora hebben we een gespecialiseerd team van deskundigen opgericht dat verantwoordelijk is voor het opsporen, analyseren en verstoren van door staatsgesponsorde en ernstige criminele cyberdreigingen. TAG traceerde Wanna Cry, de grootste ransomware-aanval in de geschiedenis, naar Noord-Korea, en deelde onlangs voorbeelden van de hack-for-hire-ecosystemen uit India, Rusland en de Verenigde Arabische Emiraten.

2010
Google Bug Hunters

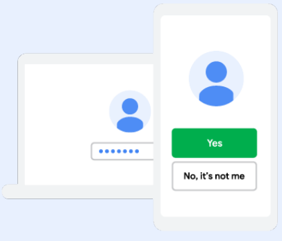
Ons Vulnerability Rewards-programma trekt via cashbeloningen middelbare scholieren, advocaten, IT-professionals en hobbyisten aan om op bugs in Google-producten op te sporen. Hun motieven zijn uiteenlopend, maar hun missie is dezelfde: onontdekte kwetsbaarheden vinden om online diensten veilig en beschermd te houden.

Miljoenen aan beloningen zijn sinds 2010 uitbetaald

2010
Red Team

Opgezet om een 'vijandige' houding aan te nemen en Google te hacken en zo te helpen onze bescherming te versterken en tekortkomingen op te sporen. Ze werken over de hele wereld om de huidige bedreigingen op de voet te volgen, beveiligingscontroles te verbeteren, aanvallen op te sporen en voorkomen, en hele klassen van kwetsbaarheden te elimineren door nieuwe en betere frameworks te ontwikkelen.

2011
Verificatie in twee stappen



We waren een van de eersten die standaard verificatie in twee stappen (2SV) aanboden en in 2021 waren we de eerste die 2SV automatisch inschakelde voor meer dan 150 miljoen mensen, waardoor ze op een veilige en eenvoudige manier konden inloggen. Zelfs als je wachtwoord is gestolen, is je account beschermd.

50% afname van gecompromitteerde accounts sinds 2SV

2013
Project Shield

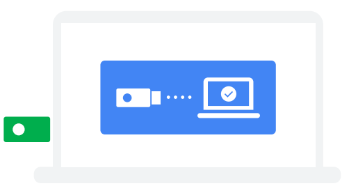
Project Shield heeft in meer dan 100 landen geholpen nieuwssites, mensenrechtenorganisaties, verkiezingssites, politieke organisaties en campagnes te beschermen tegen Distributed Denial of Service (DDoS)-aanvallen door bedreigingen te identificeren en reacties vanuit de beveiligingsgemeenschap en wetshandhaving mogelijk te maken.

150+ websites momenteel beschermd in Oekraïne

2014
Project Zero

Een gespecialiseerde taskforce die jacht maakt op zero day-kwetsbaarheden op heel het internet – in software, hardware, Google-producten en meer, om te zorgen voor een veilig en open internet. Ze waren de eersten die 'Meltdown' en 'Specter' in detail beschreven, zodat ontwikkelaars de kwetsbaarheden in CPU's snel konden aanpakken en in de hele softwareketen mitigaties konden toepassen.

2017
Geavanceerd beveiligingsprogramma (APP - Advanced Protection Program)



Extra beveiligde bescherming, inclusief de beveiligingssleutel, voor gebruikers met een hoge zichtbaarheid en een hoog risico, zoals journalisten en overheidsfunctionarissen.

300+ federale campagnes beschermd

2017
Google Play Protect

Google Play Protect is de meest gebruikte mobiele beschermingsdienst ter wereld, die zich met machinelearning van Google voortdurend aanpast en verbetert. Hiermee worden apps automatisch gescand op malware en betalingen van gebruikers op Android-telefoons worden versleuteld.

100+ miljard apps dagelijks gescand op malware

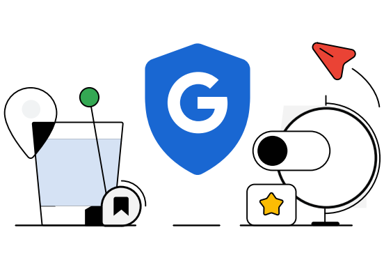
150 miljoen dagelijks versleutelde gebruikersbetalingen

2018
Titan-beveiligingssleutel

We hebben de Titan-beveiligingssleutel gemaakt voor gebruikers die een end-to-end-oplossing van Google willen. De sleutels zijn FIDO-compatibel en kunnen ook op andere plaatsen worden gebruikt, niet alleen bij Google.

2019
Wachtwoordloze herauthenticatie

Onze FIDO-ondersteuning in Android werd uitgebreid, zodat gebruikers naadloos kunnen inloggen op websites met alleen een pincode of biometrische gegevens, zonder dat daarvoor een wachtwoord nodig is.



2019
Chronicle

Chronicle is gebouwd als een gespecialiseerde laag bovenop onze kerninfrastructuur. Chronicle werd geïntroduceerd om cloudgebaseerde beveiliging te bieden, ontworpen voor ondernemingen om grote hoeveelheden beveiligings- en netwerkgegevens privé te bewaren, analyseren en doorzoeken.

2021
Investeringen om cybersecurity te bevorderen

We zetten ons in voor het versterken van cybersecurity, het uitbreiden van zero-trust-programma's, het helpen beveiligen van de leveringsketen van software en het verbeteren van de beveiliging van open source. We hebben beloofd 100.000 Amerikanen op te leiden in vakgebieden als IT-support en data-analyse via het Google Carrièrecertificaat-programma.

10 miljard dollar uitgetrokken voor Cybersecurity-initiatieven

2021
Google Open Source Security Team (GOSST)

GOSST werd opgezet om de veiligheid te verbeteren van de opensourcesoftware waarop de wereld vertrouwt. In samenwerking met de Open Source Security Foundation (OpenSSF) hebben we SLSA (Supply-Chain Levels for Software Artifacts) ontwikkeld en uitgebracht, een raamwerk om de leveringsketen van software te beschermen en langetermijnbeveiliging voor het hele software-ecosysteem mogelijk te maken.

100 miljoen dollar toegezegd aan opensource-beveiligingsoperaties van derden om kwetsbaarheden te helpen oplossen

2021
Confidential Computing

Voor de essentiële beveiliging, veiligheid en privacy hebben we Google Cloud Confidential Computing geïntroduceerd, een baanbrekende technologie die gegevens versleuteld houdt terwijl ze worden verwerkt, waardoor ze gedurende hun hele levenscyclus veilig blijven, ook wanneer ze niet gebruikt worden of verzonden/overgedragen worden. Nu kunnen zelfs de meest gevoelige gegevens met een gerust hart in de cloud worden ondergebracht.

2022
Post-Quantum Cryptography Standardization

Toekomstgericht blijven we de volgende generatie van cryptografische systemen ontwikkelen die bescherming bieden tegen inbreuk in asymmetrische cryptografie-systemen en het compromitteren van digitale communicatie. Het National Institute of Standards and Technology heeft een voorstel waarbij Google betrokken is (SPHINCS+) geselecteerd voor de standaardisering.

2022
Beschermd computergebruik

We kondigden Protected Computing aan, een groeiende toolkit van technologieën die transformeert hoe, wanneer en waar gegevens worden verwerkt waardoor de privacy en veiligheid van de gebruiker technisch worden gewaarborgd. Dit doen we door de gegevensvoetafdruk te minimaliseren, gegevens te anonimiseren en de toegang tot gevoelige gegevens te beperken. Dit betekent dat Android de volgende zin in de tekst kan suggereren, terwijl het gesprek volledig privé blijft.

2022
Mandiant en Google Cloud

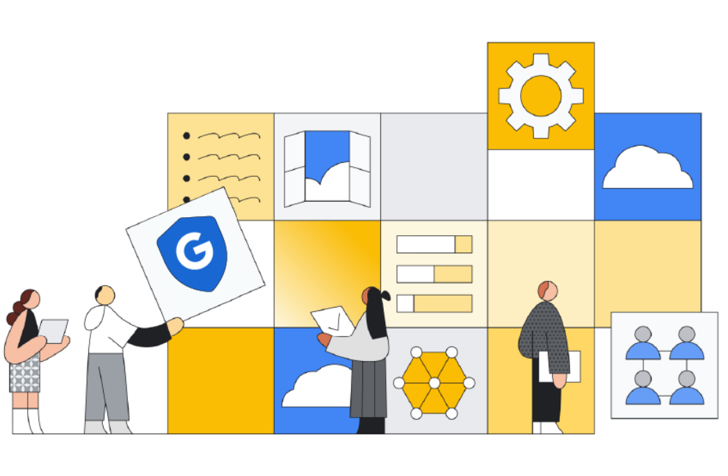
Mandiant brengt real-time, gedetailleerde informatie over bedreigingen, verkregen aan de frontlinie van cybersecurity bij de grootste organisaties ter wereld. In combinatie met het cloud-native beveiligingsaanbod van Google Cloud helpen we ondernemingen en overheidsinstellingen beschermd te blijven gedurende de gehele levenscyclus van de beveiliging.

2023
Passkey: De wachtwoordloze toekomst

We werken er al ruim tien jaar aan om de weg vrij te maken voor een toekomst zonder wachtwoorden. We hebben ons in 2013 aangesloten bij de FIDO Alliance om open standaarden voor een wachtwoordloze wereld te bewerkstelligen. Door in 2023 onze ondersteuning voor inloggen volgens FIDO-normen uit te breiden naar Android en Chrome, zullen we eindelijk kunnen beschikken over het platform voor een echt wachtwoordloze toekomst.

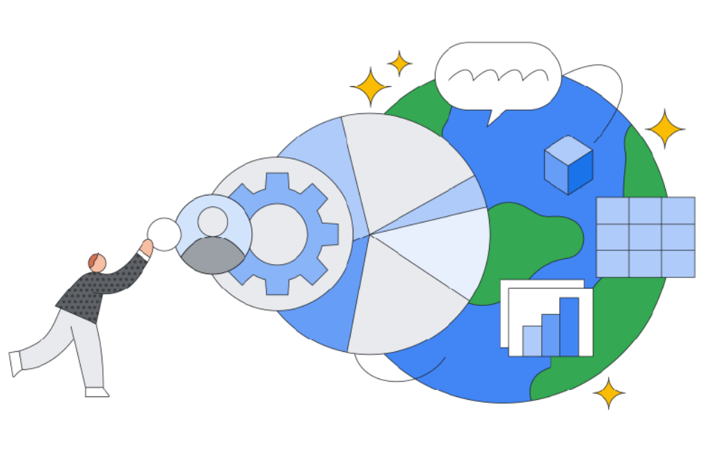
In een tijdperk van steeds uitgebreider technologisch bereik is vertrouwen in technologie de sleutel tot het ontsluiten van het ware potentieel van de samenleving.

We gaan door met het in praktijk brengen van onze beveiligingskennis en blijven ondertussen samenwerken met mensen, bedrijven en overheden om hun veiligheid te beschermen en een nieuw cybersecuritytijdperk in te luiden.



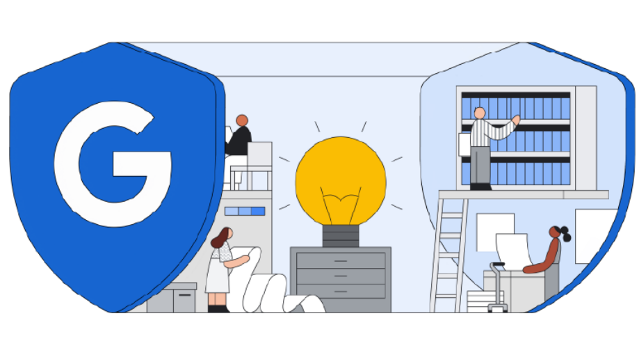
Bescherming van mensen, bedrijven en overheden

Veiligheid is de hoeksteen van onze productstrategie. Dat is waarom al onze producten ingebouwde beveiligingen hebben waardoor ze standaard veilig zijn.



De samenleving weerbaar maken tegen de veranderende dreigingen op het gebied van cybersecurity

We bieden samenlevingen de mogelijkheid om het potentieel van open source te benutten en delen onze kennis en expertise op transparante wijze met de branche om ecosystemen veiliger te houden.



Bevordering van toekomstige technologieën

We willen samenlevingen beschermen tegen de volgende generatie cyberdreigingen. Voortbouwend op onze AI-expertise ontwerpen we de volgende generatie beveiligingsarchitectuur die de grenzen van beveiligingsinnovatie verlegt.

Elke dag ben je veiliger met Google

Bezoek g.co/safety/cyber