



Vår cybersäkerhetsresa under årens lopp



Vi skyddar fler personer på nätet än någon annan i världen

Med den drastiska ökningen i antalet statsstödda cyberattacker och skadliga aktörer online anser vi att våra produkter och tjänster är mer användbara ju säkrare de är.

Vi på Google fokuserar mer än någonsin på att skydda personer, organisationer och myndigheter genom att dela med oss av våra expertkunskaper, göra det möjligt för samhället att ta itu med ständigt föränderliga cyberrisker och hela tiden arbeta på att utveckla det senaste inom cybersäkerhet så att vi kan göra [världen till en tryggare plats för alla](#).

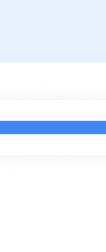


Vi utvecklar löpande och det har vi alltid gjort

Google har sedan lanseringen av Gmail 2004 varit banbrytande inom cybersäkerhetsteknik. Protected Computing som kom 2022 är ännu ett exempel. Google fortsätter att skapa nya produkter, plattformar och partnerskap för att undanröja hela klasser med hot och på så sätt skapa en säkrare framtid för personer, organisationer och samhällen. Det gör vi genom att

- ✓ utveckla säkra produkter och plattformar
- ✓ främja program och partnerskap
- ✓ sätta ihop flexibla säkerhetsteam
- ✓ finansiera innovation och utbildning till arbetsstyrkan.

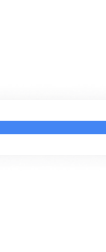
Allteftersom personers behov och internet ändras fokuserar vi på att ta fram ny teknik för att kunna stå emot de ständigt föränderliga cyberhoten. På så sätt ser vi till att varje dag är säker med Google.



2004 Skydd mot skräppost i Gmail

Vi var bland de första som tog fram AI-styrda e-postskydd.

🔍 99,9 procent av farliga och suspekta e-postmeddelanden blockerades av Gmail



2007 Säker webbsökning

Vi hjälper proaktivt till att skydda enheter runtom i världen genom att meddela användare när de besöker farliga webblätsor. De här onlineskyddna utvecklades till Förbättrad säker webbsökning 2020.

👤 5 miljarder enheter skyddas av Säker webbsökning

2009 reCAPTCHA

Vi förvärvade bedrägeri- och bothanteringslösningar för att stoppa inestoppade inloggningssuppgifter och kontouöverlåtelser och för att förhindra otillåten användning från skadliga programvaror och fälska användare.

🌐 5 miljoner webbplatser har skyddats

2008 Googles Lösenordshantering

Det blev enklare och säkrare att logga in i och med Lösenordshantering. Nu behöver man inte längre komma ihåg eller skriva in lösenord. Lösenordshantering används nu vid 50 procent av alla inloggnings i Chrome på olika plattformar.

🔑 1 miljard lösenord kontrolleras dagligen för intrång

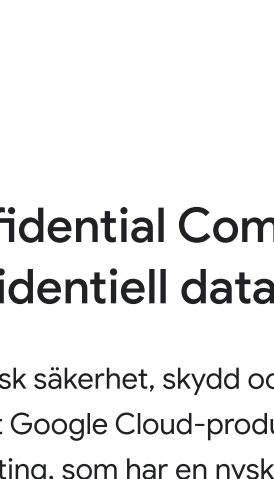
2010 Zero Trust

När vi hade överkommit Operation Aurora, som var en samordnad serie av cyberattacker, revolutionerade vi vår metod för att bygga en arkitektur som är säker som standard. Den kallas nu "Zero Trust". Vi stöttar Vita husets arbete att implementera Zero Trust-modellen i de federala myndigheterna och har också lagt in det i BeyondCorp Enterprise så att alla företag kan dra nytta av det.

2010 Threat Analysis Group (TAG)

Efter Operation Aurora satte vi ihop ett särskilt team med experter som är ansvariga för att identifiera, analysera och avbryta cybersäkerhets hot som stöds av myndigheter och allvarliga, kriminella cybersäkerhets hot. TAG spårade Wanna Cry, den största attacken med utpressningsvirus någonsin, till Nordkorea och har nyligen visat exempel på ekosystem med inhyrda hackare från Indien, Ryssland och Förenade Arabemiraten.

2010 Google Bug Hunters



Vårt belöningsprogram för de som identifierar säkerhetsrisker lockar gymnasieelever, advokater, IT-medarbetare och hobbyutvecklare att leta upp buggar i Googles produkter och få pengar för det. Anledningarna till att de gör det varierar, men målet är detsamma: hitta gömda säkerhetsrisker så att onlinetjänster är skyddade och säkra.

💰 Miljontals US-dollar har betalats ut som belöning sedan 2010

2010 The Red Team

Teamet skapades för att få in motståndarnas tankesätt med uppgiften att hacka Google så att vi kunde stärka vårt försvar och hitta luckor. De finns jorden runt och jobbar med att hålla koll på de senaste hoten, förbättra säkerhetskontroller, identifiera/förhindra attacker och eliminera hela klasser av säkerhetsrisker genom att ta fram nya och bättre ramverk.

2013 Project Shield

Project Shield har bidragit till att skydda nyhetsorganisationer, organisationer för mänskliga rättigheter, välsajter, politiska organisationer och kampanjer mot DDoS-attacker (Distributed Denial of Service) och cyberattacker i över 100 länder genom att identifiera hot och ge myndigheter och brottsbekämpande myndigheter möjlighet att bemöta.

🌐 Över 150 webbplatser skyddas av Ukraina för tillfället

2011 Tvåstegsverifiering

Vi var bland de första att erbjuda tvåstegsverifiering (2SV) som standard och först med att aktivera 2SV automatiskt för fler än 100 miljoner personer 2021. De fick därmed ett säkert och smidigt sätt att logga in. Även om någon stjal ditt lösenord är ditt konto skyddat.

🔒 50 procent färre utsatta konton sedan 2SV

2014 Project Zero

Ett särskilt team som ägnar sig åt att hitta noll dagar på internet, i programvaror, maskinvaror, Googles produkter och annat för att se till att internet är säkert och öppet. De var först med att hitta "Meltdown" och "Specter". Det gjorde det möjligt för utvecklarna att snabbt hantera CPU-brister och sätta in åtgärder i hela distributionskedjan av programvara.

2017 Advanced Protection Program (APP)

Extra säkra skydd, bland annat Säkerhetsnyckel, för användare med hög synlighet och hög risk, som journalister och myndighetspersoner.

🛡️ Mer än 300 federala kampanjer har skyddats

2018 Titan-säkerhetsnyckel

Vi skapade Titan-säkerhetsnyckeln för användare som vill ha en komplett Google-lösning. Nycklarna fungerar med FIDO och kan användas på andra ställen också, inte bara med Google.

2017 Google Play Protect

Google Play Protect är den mest implementerade skyddstjänsten för mobilt i världen. Den genomsköper automatiskt appar efter skadlig kod och krypterar användarens betalningar på Android-telefoner. Den anpassas och förbättras löpande med Googles maskininläring.

🔍 Mer än 10 miljarder appar söks igenom efter skadlig kod varje dag

🔒 150 miljoner betalningar av användare krypteras varje dag

2019 Chronicle

Chronicle byggdes för att fungera som ett särskilt lager utöver vår kärninfrastruktur och som molnbaserad säkerhet för företag så att de kunde lagra, analysera och söka i otroliga mängder säkerhets- och nätverksdata på ett skyddat sätt.

2021 Investering för att utveckla cybersäkerhet

Vi arbetar hårt för att förstärka cybersäkerheten. Det gör vi genom att utöka no-lltillitprogram, skydda distributionskedjan för programvara och förbättra säkerheten i produkterna med öppen källkod. Vi tog oss att utbilda 100 000 amerikaner i bland annat IT-säkerhet och dataanalys genom Google Karriärs certifikatprogram.

🏆 Öronmärkt 10 miljarder US-dollar till cybersäkerhetsinitiativ

2021 Confidential Computing – konfidentiell databehandling

För kritisk säkerhet, skydd och integritet har vi lanserat Confidential Computing, som har en nyskapande teknik som krypterar data medan de behandlas. På så sätt skyddas de under hela dess livscykel, både när de lagras och när de flyttas. Nu kan till och med de mest känsliga data tryggas till molnet.

2021 Google Open Source Security Team (GOSST)

GOSST skapades för att förbättra säkerheten i de öppna programvaror som många runtom i världen förlitar sig på. Vi samarbetar med Open Source Security Foundation (OpenSSF) för att utveckla och skapa SLSA (Supply-Chain Levels for Software Artifacts), ett ramverk som ska skydda distributionskedjan för programvara och säkra hela ekosystemet med programvaror på lång sikt.

💰 100 miljoner US-dollar öronmärkt till säkerhetsåtgärder med öppen källkod från andra leverantörer för att ta hand om brister

2022 Standardisering av postkvantkryptografi

Vi tänker framåt och fortsätter därför att utveckla nästa generations kryptografiska system som skyddar mot skada på kryptosystem med offentliga nycklar och inträng i digitala kommunikationssystem. National Institute of Standards and Technology har valt ut ett bidrag som Google tog del i (SPHINCS+) för standardisering.

2022 Protected Computing – skyddad databehandling

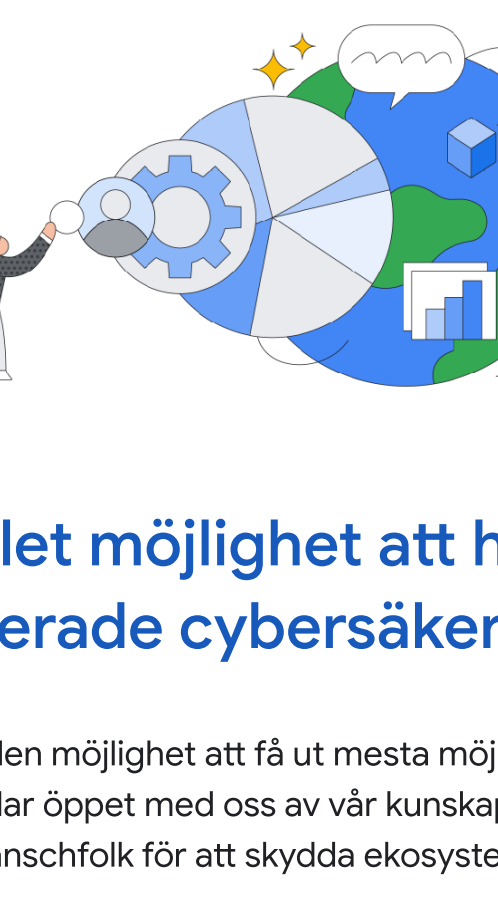
Verktygsdrivna Protected Computing, en här, när och var data behandlas för att tekniskt säkerställa att användare är skyddade och behåller sin integritet. Vi gör det här genom att minska dataavtrycket, identifiera data och begränsa åtkomst till känsliga data. Det innebär att Android kan föreslå nästa fras i en text samtidigt som konversationen är helt privat.

2023 Nyckel för en framtid utan lösenord

Vi har lagt grunden för en framtid utan lösenord i över tio år. Vi gick med i FIDO Alliance 2013 för att kunna utveckla öppna standarder för en värld utan lösenord. Vi har nu utökat vårt stöd för FIDO-inloggningsstandarder till Android och Chrome via nyckelteknik 2023 och kommer därför äntligen ha en plattform som gör att vi helt slipper lösenord i framtiden.

2022 Mandiant och Google Cloud

Med Mandiant får man ingående upplysningar om hot i realtid. Upplysningarna kommer från de största organisationerna inom cybersäkerhet i världen. Med hjälp av Google Clouds molnbaserade säkerhetslösningar hjälper vi företag och myndigheter inom den offentliga sektorn att vara skyddade under hela säkerhetslivscykeln.



I en tid där teknik hela tiden utvecklas är det viktigt att det finns tillit till den så att man kan nå samhällets fulla potential.

Vi fortsätter att samarbeta med personer, företag och myndigheter för att skydda dem och inleda en ny era inom cybersäkerhet med hjälp av våra expertkunskaper i praktiken.



Skydda personer, företag och myndigheter

Säkerhet är en hörnsten i vår produktstrategi. Det är därför alla våra produkter har inbyggda skydd som gör dem säkra som standard.

Ge samhället möjlighet att hantera allt mer avancerade cybersäkerhetsrisker

Vi ger samhällen möjlighet att få ut mesta möjliga ur öppen källkod och delar öppet med oss av vår kunskap och expertis till branschfolk för att skydda ekosystemen.

Utveckla framtidens teknik

Vi vill skydda samhällen mot nästa generation av cyberhot. Vi använder oss av våra expertkunskaper om AI och tar fram nästa våg av arkitekturen för att fortsätta innovera inom säkerhet.

Varje dag är du tryggare med Google.

Besök [g.co/safety/cyber](https://www.google.com/safety/cyber)