



Il nostro viaggio nella cybersicurezza nel corso degli anni

Più al sicuro con Google

Google si impegna ogni giorno per rendere Internet più sicuro per tutti

Con il drammatico aumento degli attacchi informatici sponsorizzati dagli Stati e delle minacce online, crediamo che i nostri prodotti e servizi siano utili solo se sicuri.

Noi di Google siamo impegnati più che mai a **proteggere** le persone, le organizzazioni e i governi condividendo le nostre competenze, mettendo la società nelle **condizioni** di affrontare i rischi informatici in continua evoluzione e lavorando continuamente per far **progredire** lo stato dell'arte della sicurezza informatica per costruire **un mondo più sicuro per tutti**.



Un'innovazione che non si ferma

Dal lancio di Gmail nel 2004 fino all'introduzione di Protected Computing nel 2022, Google ha aperto la strada alla tecnologia relativa alla cybersicurezza, continuando a innovare con prodotti, piattaforme e partnership per eliminare intere classi di minacce e creare un futuro più sicuro per le persone, le organizzazioni e le società:

- Sviluppando prodotti e piattaforme sicure
- Dando vita a team di sicurezza sempre pronti
- Promuovendo programmi e partnership
- Stanziando finanziamenti fondamentali per l'innovazione e la formazione dei dipendenti

Mentre le esigenze delle persone e di Internet si evolvono, noi continuiamo a proporre tecnologie all'avanguardia per mitigare le minacce informatiche in continuo cambiamento, assicurandoci che ogni giorno sia più sicuro insieme a Google.

2004 Protezione dallo spam di Gmail

Siamo stati tra i primi a creare filtri antispam per le e-mail basati sull'intelligenza artificiale.

Il **99.9%** delle e-mail pericolose o sospette viene **bloccato** da Gmail

2007 Navigazione sicura

Contribuiamo attivamente a proteggere i dispositivi di tutto il mondo avvisando gli utenti quando visitano siti web pericolosi, e nel 2020 abbiamo fatto evolvere ulteriormente queste protezioni online con **Navigazione sicura avanzata**.

5 miliardi di dispositivi **protetti** da Navigazione sicura

2009 reCAPTCHA

Abbiamo acquisito la soluzione di gestione di frodi e bot per interrompere pratiche come credential stuffing e violazioni di account, e per prevenire attività illecite da agenti malintenzionati come software e utenti falsi.

5 milioni di siti web **difesi**

2008 Gestore delle password di Google

L'introduzione di Gestore delle password ha reso l'accesso più semplice e sicuro, senza la necessità di ricordare o digitare la password. Oggi è utilizzato per il 50% di tutti i login su Chrome nelle varie piattaforme.

1 miliardo di password **controllate** ogni giorno per verificare la presenza di violazioni

2010 Zero Trust

Dopo la difficile esperienza dell'Operazione Aurora, una serie coordinata di **attacchi informatici**, abbiamo rivoluzionato il nostro approccio per costruire un'architettura "secure by default" ora nota come "Zero Trust", che garantisce meno vettori di attacco, meno opportunità di perdere dati e più controllo sui sistemi da cui dipendono gli utenti. Sosteniamo l'impegno della Casa Bianca per diffondere il modello Zero Trust in tutto il governo federale e lo abbiamo anche inserito in BeyondCorp Enterprise in modo che qualsiasi azienda possa sfruttarlo.

2010 Threat Analysis Group (TAG)

Dopo l'Operazione Aurora, abbiamo formato un team specializzato di esperti incaricato di rilevare, analizzare e fermare le minacce informatiche sostenute dai governi e dai criminali. TAG ha fatto risalire Wanna Cry, il più grande attacco ransomware della storia, alla Corea del Nord e ha recentemente condiviso **esempi** di ecosistemi di hack-for-hire provenienti da India, Russia ed Emirati Arabi Uniti.

2010 Google Bug Hunters

Il nostro programma Vulnerability Rewards attira studenti di scuole superiori, avvocati, professionisti IT e appassionati affinché vadano a caccia di bug nei prodotti Google, ricevendo in cambio premi in denaro. I "cacciatori" possono essere spinti da motivi diversi, ma la loro missione è la stessa: trovare vulnerabilità nascoste per mantenere i servizi online al sicuro.

Milioni di dollari destinati ai premi dal 2010

2010 The Red Team

Lanciato per adottare una mentalità antagonista e rafforzare le nostre difese e a individuare eventuali lacune. Il Red Team opera in tutto il mondo per rimanere al passo con le minacce attuali, migliorare i controlli di sicurezza, condurre il rilevamento/la prevenzione degli attacchi ed eliminare intere classi di vulnerabilità, creando framework nuovi e migliori.

2013 Project Shield

Project Shield ha contribuito a proteggere l'informazione, le organizzazioni per i diritti umani, i siti elettorali, le organizzazioni politiche e le campagne elettorali da attacchi informatici DDoS (Distributed Denial of Service) in oltre 100 Paesi, identificando le minacce e consentendo agli esperti di sicurezza e alle forze dell'ordine di reagire.

Oltre **150+** siti web **protetti** al momento in Ucraina

2011 Verifica in due passaggi

Siamo stati tra i primi a offrire la Verifica in due passaggi (2SV) di default, e i primi ad abilitare automaticamente la 2SV per oltre 150 milioni di persone nel 2021, fornendo una modalità di accesso semplice e sicura. Anche se la tua password viene compromessa, il tuo account rimane protetto.

Diminuzione del **50%** degli account compromessi da quando esiste la 2SV

2014 Project Zero

Una task force specializzata, dedicata all'individuazione delle minacce zero day in tutto Internet, nei software, nell'hardware, nei prodotti Google e oltre, per garantire un'Internet sicura e aperta. Sono stati i primi a descrivere "Meltdown" e "Specter", consentendo agli sviluppatori di affrontare rapidamente le vulnerabilità delle CPU e di applicare le correzioni necessarie in tutta la catena di fornitura del software.

2017 Advanced Protection Program (APP)

Protezioni ultrasicure, inclusi i token di sicurezza, per utenti in primo piano e ad alto rischio, come giornalisti e funzionari governativi.

Oltre **300+** campagne federali **protette**

2018 Token di sicurezza Titan

Abbiamo creato il token di sicurezza Titan per gli utenti che desiderano una soluzione end-to-end di Google. I token sono realizzati sulla base degli standard FIDO e possono essere utilizzati anche altrove, non solo con Google.

2019 Ri-autenticazione senza password

Abbiamo esteso il supporto FIDO su Android, in modo che gli utenti potessero accedere ai siti web facilmente con un semplice PIN o un'autenticazione biometrica, senza bisogno di password.

2017 Google Play Protect

Google Play Protect è lo strumento più diffuso al mondo per proteggere i dispositivi mobili da potenziali minacce. Si adatta e migliora costantemente grazie all'apprendimento automatico di Google, analizza automaticamente le app alla ricerca di malware e crypta i pagamenti degli utenti sui telefoni Android.

+100 miliardi di app analizzate alla ricerca di malware ogni giorno

150 milioni di pagamenti **criptati** ogni giorno

2019 Chronicle

Costruito come un livello specializzato in aggiunta alla nostra infrastruttura principale, Chronicle è stato introdotto per garantire sicurezza e permettere alle aziende di conservare, analizzare e cercare privatamente enormi quantità di dati relativi alla sicurezza e alle reti.

2021 Investimenti per la sicurezza informatica

Il nostro impegno è quello di rafforzare la sicurezza dei software open source, espandere il nostro trust, contribuire alla sicurezza della catena di fornitura dei software e migliorare la sicurezza dell'open source.

10 miliardi di dollari stanziati per iniziative di cybersicurezza

2021 Confidential Computing

Per questioni critiche legate alla sicurezza e alla privacy, abbiamo introdotto Google Cloud Confidential Computing, una tecnologia all'avanguardia che mantiene i dati crittografati durante l'elaborazione e che permette di tenerli al sicuro durante l'intero ciclo di vita, anche quando sono a riposo o in transito. Ora è possibile effettuare la migrazione sul cloud anche dei dati più sensibili.

2021 Google Open Source Security Team (GOSST)

Il GOSST è stato creato per migliorare la sicurezza dei software open source su cui il mondo fa affidamento. Abbiamo collaborato con la Open Source Security Foundation (OpenSSF) per sviluppare e lanciare il Supply-Chain Levels for Software Artifacts (SLSA), un framework per proteggere la catena di fornitura dei software e assicurare a lungo termine la sicurezza dell'intero ecosistema del software.

100 milioni di dollari stanziati per operazioni di sicurezza open source di terze parti per risolvere le vulnerabilità

2022 Standardizzazione della crittografia post-quantistica

Con uno sguardo sempre rivolto al futuro, continuiamo a sviluppare sistemi crittografici di nuova generazione in grado di contrastare la violazione dei sistemi crittografici a chiave pubblica e la compromissione delle comunicazioni digitali. Il National Institute of Standards and Technology ha selezionato una proposta di standardizzazione con il coinvolgimento di Google (SPHINCS+).

2022 Protected Computing

Abbiamo annunciato Protected Computing, un insieme in continua crescita di tecnologie in grado di trasformare le modalità, i tempi e i luoghi di elaborazione dei dati per garantire tecnicamente la privacy e la sicurezza dei dati degli utenti. Lo facciamo minimizzando l'impronta dei dati, rendendoli anonimi e limitando l'accesso ai dati sensibili. Ciò significa che Android può suggerire la prossima parola nei messaggi, ma le conversazioni rimangono del tutto private.

2023 Passkey, per un futuro senza password

Da oltre dieci anni stiamo lavorando a un futuro senza password. Abbiamo aderito alla FIDO Alliance nel 2013 per promuovere standard aperti per un mondo senza password e ora, espandendo il supporto agli standard di autenticazione FIDO ad Android e Chrome con la tecnologia passkey nel 2023, avremo finalmente la piattaforma che ci porterà un futuro davvero senza password.

2022 Mandiant e Google Cloud

Mandiant offre un'approfondita intelligenza sulle minacce in tempo reale, acquisita in prima linea con le più grandi organizzazioni del mondo. Insieme alle funzioni di sicurezza di Google Cloud, aiutiamo le aziende e gli enti pubblici a rimanere protetti durante l'intero ciclo di vita della sicurezza.



In un periodo in cui la portata tecnologica è in continua espansione, la fiducia nella tecnologia è essenziale per sbloccare il vero potenziale della società.

Mettendo in pratica le nostre conoscenze in materia di sicurezza, continueremo a collaborare con le persone, le aziende e i governi per tenerli al sicuro e guidare una nuova era nella cybersicurezza.



Proteggiamo le persone, le aziende e i governi

Alla base della nostra strategia di prodotto c'è la sicurezza. È per questo che tutti i nostri prodotti sono dotati di protezioni integrate che li rendono sicuri di base.

Mettiamo la società nelle condizioni di affrontare i rischi continui della cybersicurezza

Mettiamo le società nelle condizioni di scoprire il potenziale dell'open source e condividiamo in modo trasparente le nostre conoscenze e competenze con il settore per rendere gli ecosistemi più sicuri.

Lavoriamo alle tecnologie del futuro

Vogliamo proteggere le società dalle minacce informatiche del futuro. Basandoci sulla nostra esperienza nell'IA, stiamo progettando le prossime architetture per spingere i confini dell'innovazione della sicurezza.

Più sicurezza online con Google ogni giorno

Visita g.co/safety/cyber