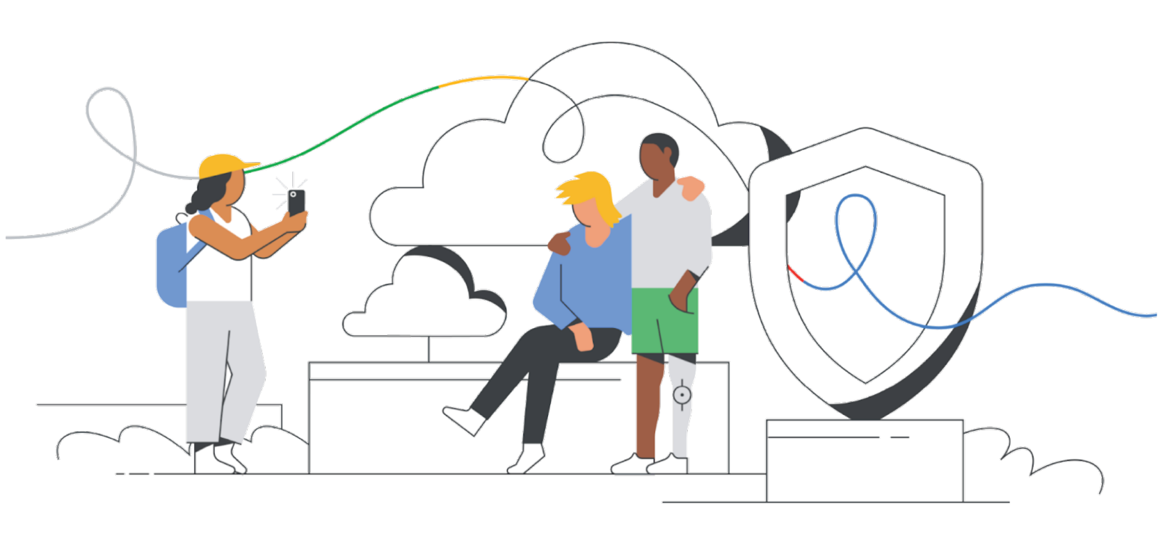
Our cybersecurity journey through the years

Safer with Google

We keep more people safe online than anyone else in the world

With the dramatic rise of state-sponsored cyber attacks and malicious actors online, we believe our products and services are only as helpful as they are secure.

At Google, we are more focused than ever on protecting people, organizations and governments by sharing our expertise, empowering the society to address ever-evolving cyber risks and continuously working to advance the state of the art in cybersecurity to build a safer world for everyone.



Continuously innovating through the ages

Since the launch of Gmail in 2004 to the introduction of Protected Computing in 2022, Google has been pioneering cybersecurity technology and continually innovating on products, platforms, and partnerships to eliminate entire classes of threats to create a safer future for people, organizations and societies by:

- ✓ Developing secure products and platforms
- ✓ Building agile Security Teams
- ✓ Fostering programs and partnerships
- ✓ Providing critical funding for innovation and workforce training

As people's needs and the internet evolve, we continue to be at the forefront of new technologies to mitigate ever-changing cyberthreats, ensuring that every day is safer with Google.

2004
Gmail Spam Protection

We were one of the first to build AI-driven email protections.

99.9% of dangerous and suspicious emails are blocked by Gmail

2007
Safe Browsing

We help proactively protect devices around the world by alerting users when they visit dangerous websites, evolving these online protections into Enhanced Safe browsing in 2020.

5 Billion devices protected by Safe Browsing

2009
reCAPTCHA

We acquired the fraud and bot management solution to stop credential stuffing and account takeovers, and to prevent abusive activities from malicious software/fake users.

5 Million websites defended

2008
Google Password Manager

The introduction of Password Manager made signing-in easier and safer, without the need to remember or type in your password and is now used for 50% of all logins in Chrome across platforms.

1 Billion passwords checked daily for breaches

2010
Zero Trust

After surviving Operation Aurora, a coordinated series of cyber attacks, we revolutionized our approach to build a secure-by-default architecture now known as "Zero Trust". It ensures fewer attack vectors, fewer opportunities to lose data, and more control over the systems users depend on. We support the White House's efforts to deploy the Zero Trust model across the federal government and have also packaged it into BeyondCorp Enterprise so that any enterprise can leverage it.

2010
Threat Analysis Group (TAG)

After Operation Aurora, we formed a specialized team of experts responsible for detecting, analyzing, and disrupting government-backed and serious criminal cyber threats. TAG traced Wanna Cry, the largest ransomware attack in history, to North Korea, and recently shared examples of the hack-for-hire ecosystems from India, Russia, and the United Arab Emirates.

2010
Google Bug Hunters

Our Vulnerability Rewards program attracts high schoolers, lawyers, IT professionals, and hobbyists to hunt down bugs in Google products with cash prizes. Their motives vary, but their mission is the same: find undiscovered vulnerabilities to keep online services safe and secure.

Millions of dollars paid out in rewards since 2010

2010
The Red Team

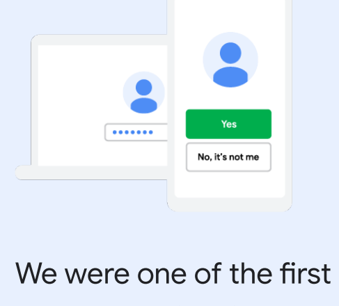
Launched to take on an adversarial mindset and hack Google to help strengthen our defenses and spot gaps. They work across the globe to keep up with current threats, improve security controls, conduct attack detection/prevention, and eliminate entire classes of vulnerabilities by driving new and better frameworks.

2013
Project Shield

Project Shield has helped protect news, human rights organizations, election sites, political organizations, and campaigns from Distributed Denial of Service (DDoS) attacks in over 100 countries from cyber attacks by identifying threats and enabling responses in the security community and law enforcement.

150+ websites currently protected in Ukraine

2011
2-Step Verification



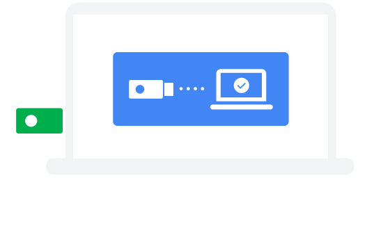
We were one of the first to offer 2-Step Verification (2SV) by default, and the first to auto-enable 2SV for over 150 million people in 2021, providing a safe and easy way to log in. Even if your password is stolen, your account is protected.

50% decrease in compromised accounts since 2SV

2014
Project Zero

A specialized task force devoted to hunting zero day exploits across the internet - in software, hardware, Google products, and beyond to ensure a safe and open Internet. They were the first to detail "Meltdown" and "Specter," enabling developers to quickly address CPU vulnerabilities and apply mitigations across the software supply chain.

2017
Advanced Protection Program (APP)



Extra secure protections, including Security Key, for high-visibility and high-risk users such as journalists and government officials.

300+ federal campaigns protected

2018
Titan Security Key

We made the Titan Security Key for users who want an end-to-end Google solution. The keys are FIDO compliant and can be used elsewhere too, not just with Google.

2019
Passwordless Re-Authentication

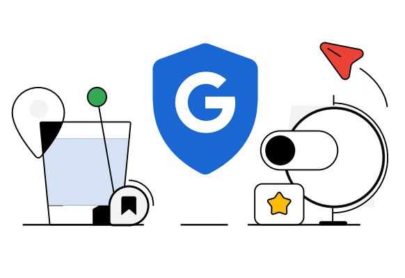
Extended our FIDO support in Android so users could seamlessly log on to websites with just a PIN or biometric, no password needed.

2017
Google Play Protect

The most widely deployed mobile threat protection service in the world, constantly adapting and improving with Google's machine learning, Google Play Protect automatically scans apps for malware and encrypts user payments on Android phones.

100+ Billion apps scanned for malware daily

150 Million user payments encrypted daily



2019
Chronicle

Built as a specialized layer on top of our core infrastructure, Chronicle was introduced to provide cloud-based security designed for enterprises to privately retain, analyze, and search massive amounts of security and network data.

2021
Investment to Advance Cybersecurity

We're committed to strengthening cybersecurity, expanding zero-trust programs, helping secure the software supply chain, and enhancing open-source security. We pledged to train 100,000 Americans in fields like IT Support and Data Analytics through the Google Career Certificate program.

$10 Billion commitment to cybersecurity initiatives

2021
Confidential Computing

For critical security, safety, and privacy, we introduced Google Cloud Confidential Computing, a breakthrough technology that keeps data encrypted while it is being processed, allowing it to stay secure throughout its entire life cycle, including while at rest or in transit. Now even the most sensitive data can confidently be migrated to the cloud.

2021
Google Open Source Security Team (GOSST)

GOSST was created to improve the security of the open source software the world relies on. We partnered with the Open Source Security Foundation (OpenSSF) to develop and release Supply-Chain Levels for Software Artifacts (SLSA), a framework to secure the software supply chain and enable long-term security for the entire software ecosystem.

$100 Million committed to third party open source security operations to help fix vulnerabilities

2022
Post-Quantum Cryptography Standardization

Future focused, we continue to develop next-generation cryptographic systems that safeguard against the breaking of public-key cryptosystems and compromising digital communications. The National Institute of Standards and Technology selected a submission with Google's involvement (SPHINCS+) for standardization.

2022
Protected Computing

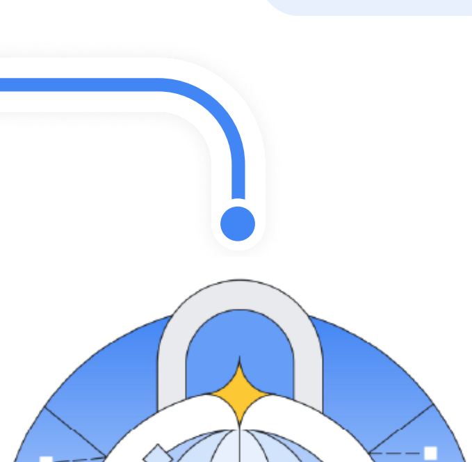
We announced Protected Computing, a growing toolkit of technologies that transforms how, when, and where data is processed to technically ensure user's privacy and safety. We do this by minimizing the data footprint, de-identifying data, and restricting access to sensitive data. This means Android can suggest the next phrase in the text, while keeping the conversation completely private.

2023
Passkey: The Passwordless Future

We've been setting the stage for a passwordless future for over a decade. We joined the FIDO Alliance in 2013 to drive open standards for a passwordless world and now by expanding our support for FIDO Sign-in standards to Android & Chrome through passkey technology in 2023, we will finally have the platform for a truly passwordless future.

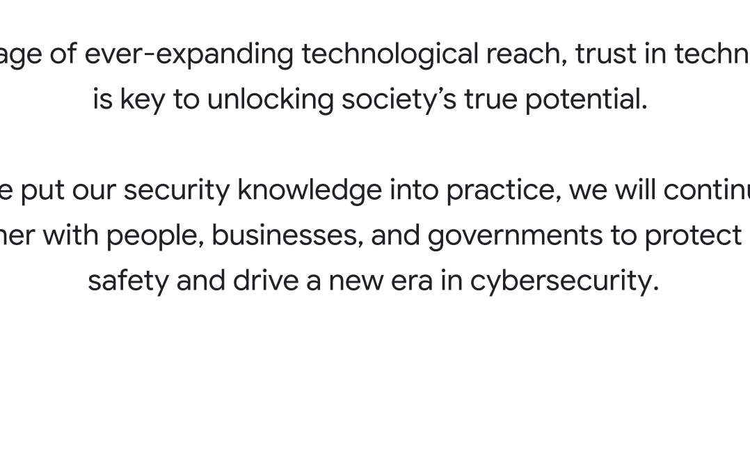
2022
Mandiant and Google Cloud

Mandiant brings real-time, in-depth threat intelligence gained on the frontlines of cybersecurity with the largest organizations in the world. Combined with Google Cloud's cloud-native security offerings, we help enterprises and public sector agencies stay protected throughout the security lifecycle.



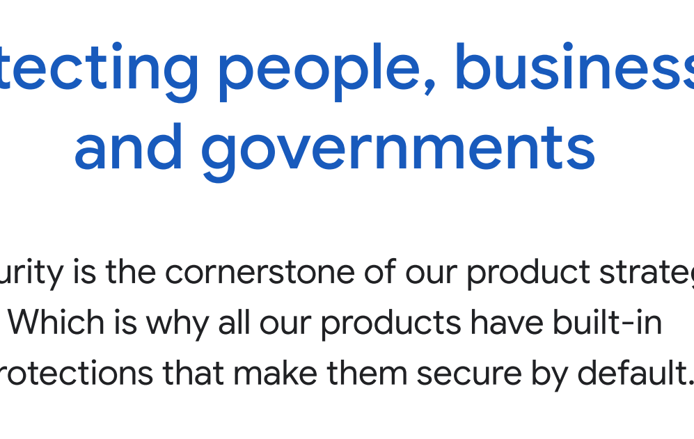
In an age of ever-expanding technological reach, trust in technology is key to unlocking society's true potential.

As we put our security knowledge into practice, we will continue to partner with people, businesses, and governments to protect their safety and drive a new era in cybersecurity.



Protecting people, businesses and governments

Security is the cornerstone of our product strategy. Which is why all our products have built-in protections that make them secure by default.



Empowering society to address evolving cybersecurity risks

We empower societies to unlock the potential of open source, and share our knowledge and expertise transparently with the industry to keep ecosystems safer.

Advancing future technologies

We want to protect societies from the next generation of cyberthreats. Building on our AI expertise, we are designing the next wave of architectures to push the boundaries of security innovation.

Every day you're safer with Google

Visit g.co/safety/cyber