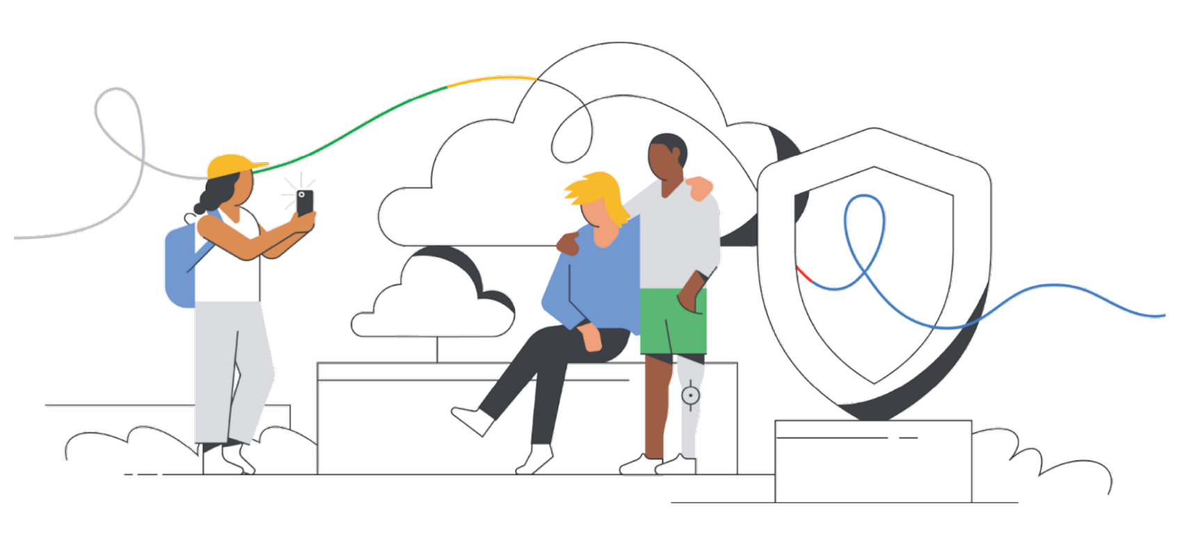
Cybersecurity bei Google

Besser geschützt mit Google

Wir arbeiten kontinuierlich daran, dass die Menschen in Deutschland online geschützt sind

Angesichts der dramatischen Zunahme staatlich gesponsorter Cyberangriffe und böswilliger Akteure im Internet sind wir davon überzeugt, dass unsere Produkte und Dienstleistungen sicher sein müssen, damit sie den Menschen helfen.

Für uns bei Google ist Sicherheit ein zentraler Pfeiler unserer Produktentwicklung, entsprechend ist es uns wichtig, dass unsere Produkte durch standardmäßige Sicherheitsfunktionen geschützt sind. Wir verfolgen einen offenen und transparenten Ansatz in Bezug auf Sicherheit, teilen unser Wissen und arbeiten aktiv mit Branchenpartnern, Regierungen und der Gesellschaft zusammen, um moderne Sicherheitslösungen für alle anzubieten.



Kontinuierliche Innovation im Wandel der Zeit

Seit dem Launch von Gmail im Jahr 2004 bis hin zur Einführung von Protected Computing im Jahr 2022 leistet Google Pionierarbeit im Bereich der Cybersicherheitstechnologie und entwickelt ständig neue Produkte, Plattformen und Partnerschaften. Dabei setzen wir uns dafür ein, Cyberbedrohungen zu beseitigen und eine sicherere Zukunft für Gesellschaft, Wirtschaft, Staat und Verwaltung zu schaffen:

- ✓ Entwicklung von Schutzmechanismen für Produkte und Plattformen
- ✓ Aufbau von agilen Sicherheitsteams
- ✓ Förderung von Programmen und Partnerschaften
- ✓ Bereitstellung von wichtigen Förderungen für Innovationen und Arbeitnehmerschulung

Da sich die Bedürfnisse der Menschen und das Internet immer wieder wandeln, entwickeln wir kontinuierlich neue Technologien, um die sich ständig ändernden Cyberbedrohungen zu minimieren und sicherzustellen, dass mit Google jeder Tag sicherer ist.

2004
Spamschutz in Gmail

Wir waren die Ersten, die E-Mails mit KI-gesteuerten Sicherheitsfunktionen verknüpft haben.

99,9% der gefährlichen oder verdächtigen E-Mails werden von Gmail blockiert

2007
Safe Browsing

Wir helfen dabei, Geräte auf der ganzen Welt proaktiv besser zu schützen, indem wir Nutzer:innen warnen, wenn sie gefährliche Websites besuchen. Im Jahr 2020 wurden diese Online-Schutzmaßnahmen zum Erweiterten Safe Browsing weiterentwickelt.

5 Milliarden Geräte werden durch Safe Browsing geschützt

2009
reCAPTCHA

Wir haben die Betrugs- und Bot-Management-Lösung reCAPTCHA erworben, um den Diebstahl von Anmeldeinformationen und die Übernahme von Konten zu unterbinden und missbräuchliche Aktivitäten böswilliger Software bzw. gefälschter Nutzerkonten zu verhindern.

5 Millionen Websites werden besser geschützt

2008
Google Passwortmanager

Die Einführung des Passwortmanagers hat Anmeldungen einfacher und sicherer gemacht, ohne dass sich Nutzer:innen Passwörter merken oder sie eintippen müssen. Das Tool wird aktuell plattformübergreifend für 50 % aller Anmeldungen in Chrome verwendet.

1 Milliarde Passwörter werden täglich überprüft

2010
Zero Trust

Nachdem wir Operation Aurora, eine koordinierte Reihe an Cyberangriffen, überstanden hatten, revolutionierten wir unseren Ansatz und bauten eine standardmäßig geschützte Architektur auf – die „Zero-Trust-Architektur". Sie verringert die Angriffsvektoren und die Arten, auf die Daten verloren gehen können. Zusätzlich bietet sie mehr Sicherheit über die von Nutzer:innen benötigten Systeme hinweg. Diese Architektur haben wir auch in BeyondCorp Enterprise integriert, damit sie von jedem Unternehmen genutzt werden kann.

2010
Threat Analysis Group (TAG)

Nach der Operation Aurora haben wir ein spezialisiertes Expertenteam für die Erkennung, Analyse und Abwehr staatlich gesteuerter und krimineller Cyberbedrohungen gebildet. Die TAG verfolgte die Spur von Wanna Cry, dem größten Ransomware-Angriff der Geschichte, nach Nordkorea. Kürzlich teilte sie außerdem auch Beispiele für die Hack-for-Hire-Ökosysteme aus Indien, Russland und den Vereinigten Arabischen Emiraten.

2010
Google Bug Hunters

Unser Vulnerability Rewards-Programm animiert Schüler:innen, Jurist:innen sowie Menschen mit besonderen oder wenigen IT Kenntnissen mit Geldprämien dazu, nach Fehlern in Google-Produkten zu suchen. Die Motive der Teilnehmer:innen sind unterschiedlich, aber ihre Mission ist die gleiche: unentdeckte Schwachstellen zu finden, um Online-Dienste sicherer zu machen.

Mehrere Millionen Dollar wurden in diesem Zusammenhang seit 2010 als Belohnungen ausgezahlt

2010
Das „Red Team"

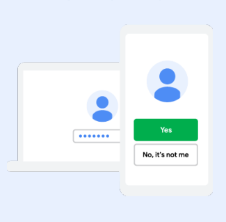
Gegründet, um die Sicht eines Angreifers anzunehmen, versucht das Red Team, Google zu hacken, damit wir unsere Produkte verbessern und Schwachstellen erkennen können. Das Team arbeitet weltweit daran, mit aktuellen Bedrohungen Schritt zu halten, Sicherheits-Checks zu verbessern, Angriffe zu erkennen und zu verhindern sowie Sicherheitslücken durch die Entwicklung neuer und besserer Systeme zu beseitigen.

2013
Project Shield

Das Project Shield hat dazu beigetragen, Nachrichten, Menschenrechtsorganisationen, Wahlen, politische Organisationen und Kampagnen in über 100 Ländern vor DDoS-Angriffen (Distributed Denial of Service) zu schützen, indem es Bedrohungen identifiziert und so Reaktionen der Sicherheitsgemeinschaft und der Strafverfolgungsbehörden ermöglicht.

Über 150 Websites werden aktuell in der Ukraine besser geschützt

2011
2-Stufen-Verifizierung



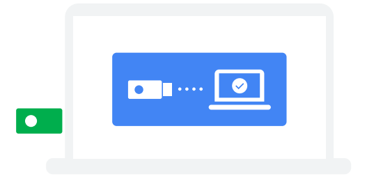
Wir waren eines der ersten Unternehmen, das standardmäßig die Zwei-Faktor-Authentifizierung (2SV) angeboten hat und das erste Unternehmen, das 2021 die 2SV automatisch für über 150 Millionen Menschen aktiviert hat, um Anmeldungen sicherer und einfacher zu machen. Damit können Nutzer:innen Ihr Konto besser schützen, selbst wenn ein Passwort kompromittiert wurde.

50 % Rückgang der Probleme mit Konten seit der Einführung von 2SV

2014
Project Zero

Eine spezialisierte Task Force, die zur Gewährleistung eines sicheren und offenen Internets nach Zero-Day-Exploits in Soft- und Hardware sowie in Google-Produkten sucht. Sie haben „Meltdown" und „Specter" erstmals detailliert beschrieben und ermöglichen es Entwickler:innen, CPU-Schwachstellen schnell zu beheben und Abhilfemaßnahmen auf die gesamte Software-Lieferkette anzuwenden.

2017
Erweitertes Sicherheitsprogramm



Der zusätzliche Schutz, zum Beispiel über einen Sicherheitsschlüssel für Nutzer:innen mit erhöhtem Risiko für Onlineangriffe, darunter Menschen, die in den Bereichen Journalismus und Regierung arbeiten, wurde erweitert.

2018
Titan-Sicherheitsschlüssel

Wir haben den Titan-Sicherheitsschlüssel für Nutzer:innen entwickelt, die sich noch mehr Schutz vor Phishing und Konto-Hacking wünschen. Die Schlüssel sind FIDO-konform und können auch außerhalb von Google Produkten verwendet werden.

2019
Passwortfreie Re-Authentifizierung

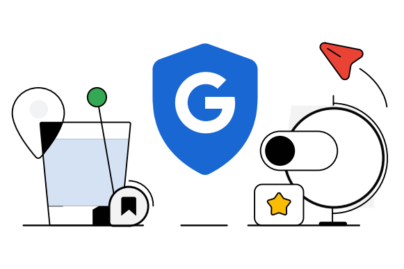
Wir haben unsere FIDO-Unterstützung in Android erweitert, sodass sich Nutzer:innen nun mit nur einer PIN oder biometrisch auf Websites anmelden können, ohne ein Passwort eingeben zu müssen.

2017
Google Play Protect

Google Play Protect ist der weltweit am weitesten verbreitete Dienst zum Schutz vor mobilen Bedrohungen. Dank des maschinellen Lernens von Google passt er sich ständig an und verbessert sich. Google Play Protect scannt Apps automatisch auf Malware und verschlüsselt Nutzerzahlungen auf Android-Handys.

Über 100 Milliarden Apps werden täglich auf Malware gescannt

150 Millionen Nutzerzahlungen werden täglich verschlüsselt



2019
Chronicle

Chronicle wurde als spezialisierte Schicht auf unserer Kerninfrastruktur aufgesetzt und bietet Cloud-basierte Sicherheit für Unternehmen, die große Mengen an Sicherheits- und Netzwerkinformationen aufbewahren, analysieren und durchsuchen.

2021
Investition zur Förderung der Cybersecurity

Wir engagieren uns dafür, die Cybersecurity zu stärken, Zero-Trust-Programme auszuweiten, Software-Lieferketten besser zu sichern und die Open-Source-Sicherheit zu verbessern.
In diesem Rahmen vergeben wir u.a. in Europa, dem Mittleren Osten und Afrika 150.000 Stipendien für flexible Online-Kurse, sogenannte "Google Career Certificates". In den Kursen können sich Teilnehmende berufsqualifizierende Kompetenzen in IT-Support, Datenanalyse, UX Design und Projektmanagement kostenlos aneignen.

$ 10 Milliarden für Initiativen im Bereich der Cybersecurity

2021
Confidential Computing

Für kritische Sicherheit und Datenschutz haben wir Google Cloud Confidential Computing entwickelt. Dank dieser neuen Technologie werden Informationen während der Verarbeitung bestmöglich verschlüsselt. So können auch sensible Daten in die Cloud migriert werden.

2021
Google Open Source Security Team (GOSST)

GOSST wurde gegründet, um die Sicherheit global verwendeter Open-Source-Software zu verbessern. Gemeinsam mit der Open Source Security Foundation (OpenSSF) haben wir die Supply-Chain Levels for Software Artifacts (SLSA) entwickelt und veröffentlicht. Dieses Sicherheits-Framework soll die Software-Lieferkette schützen und langfristige Sicherheit für das gesamte Software-Ökosystem ermöglichen.

$ 100 Millionen wurden Open-Source-Sicherheitsoperationen von Dritten zur Verfügung gestellt, um Schwachstellen zu beseitigen

2022
Post-Quantum Cryptography Standardization

Wir entwickeln mit Blick auf die Zukunft neue kryptografische Systeme, um dem Zusammenbruch von Kryptosystemen mit öffentlichen Schlüsseln und der Beeinträchtigung der digitalen Kommunikation entgegenzuwirken.

2022
Protected Computing

Wir haben Protected Computing entwickelt, eine wachsende Palette von Technologien, die verändern, wie, wann und wo Informationen verarbeitet werden, um so Privatsphäre und Sicherheit der Nutzer:innen bestmöglich zu schützen. Dabei ist es uns wichtig, den Daten-Fußabdruck zu minimieren, Informationen zu anonymisieren und den Zugriff auf sensible Inhalte zu beschränken.
In diesem Zusammenhang kann zum Beispiel Android einen Vorschlag für Textnachrichten machen, obwohl die Konversation geschützt ist.

2023
Passkey: Die passwortfreie Zukunft

Seit über einem Jahrzehnt stellen wir die Weichen für eine passwortfreie Zukunft. Wir sind 2013 der FIDO Alliance beigetreten, um offene Standards für eine passwortlose Welt voranzutreiben. Da wir 2023 unsere Unterstützung für FIDO-Anmeldestandards auf Android und Chrome durch die Passkey-Technologie ausweiten, haben wir endlich eine Plattform für eine wirklich passwortfreie Zukunft.

2022
Mandiant und Google Cloud

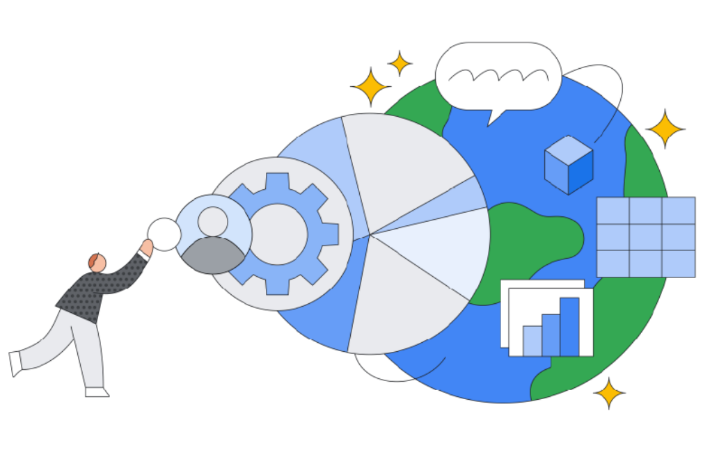
Mandiant verfügt über detaillierte Bedrohungsdaten in Echtzeit, die an der Front der Cybersecurity bei den weltweit größten Organisationen gewonnen werden. In Kombination mit den Cloud-nativen Sicherheitsangeboten von Google Cloud helfen wir so Unternehmen und Behörden, während des gesamten Sicherheitslebenszyklus besser geschützt zu sein.

In einer Zeit, in der sich die technologischen Möglichkeiten immer weiter entwickeln, ist Vertrauen in Technologie der Schlüssel dafür, das wahre Potenzial der Gesellschaft zu entfalten.

Während wir unsere Sicherheitsexpertise in die Praxis umsetzen, kooperieren wir weiter mit Regierungen, Unternehmen sowie Nutzer:innen, um sie besser zu schützen und damit als Pionier das Thema "Cybersecurity" voranzutreiben.

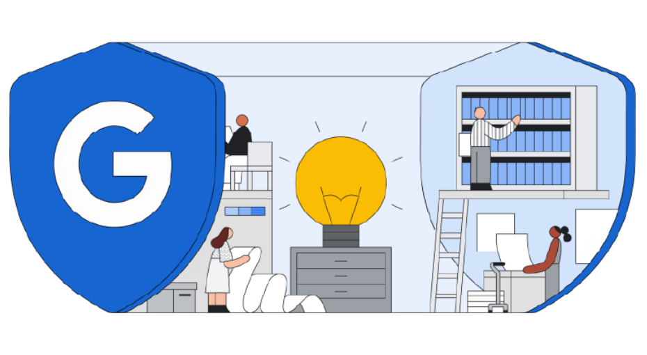
Mehr Onlinesicherheit - für Gesellschaft, Wirtschaft, Staat und Verwaltung

Integrierte Sicherheit ist das Fundament unserer Produktstrategie. All unsere Produkte verfügen standardmäßig über moderne Schutzmechanismen, die erhöhte Sicherheit gewährleisten.



Für ein offenes und vertrauenswürdiges Internet

Als Internet-Unternehmen sind uns die Grundprinzipien des Internets wichtig: Offenheit und Interoperabilität. Wir teilen unser Wissen und unsere Expertise mit der Branche und stellen viele unserer Technologien als Open Source zur Verfügung, um für alle höhere Sicherheitsstandards zu etablieren.



Führend im Bereich Cybersecurity

Unser Ziel: Menschen vor zunehmenden Cyberbedrohungen zu schützen und somit das Internet für alle sicherer zu machen.

Jeden Tag online besser geschützt mit Google

Erfahren Sie mehr unter
safety.google