Google

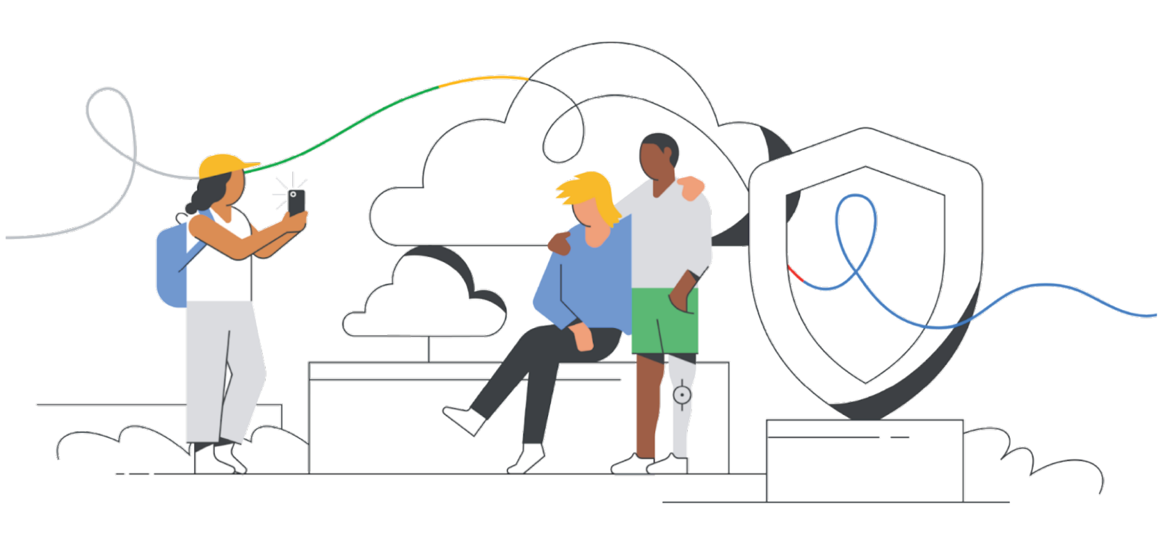
수년간의 사이버 보안 여정

Safer with Google

Google은 온라인상의 많은 이용자를 안전하게 보호하기 위해 매일 노력합니다.

국가 주도의 사이버 공격과 악의적인 온라인 이용자들이 급증하는 오늘날,
Google 제품 및 서비스의 뛰어난 보안 수준은
이용자를 안전하게 보호하는 데 도움을 줍니다.

Google은 이용자, 조직 및 정부를 보호하는 데 그 어느 때보다 주력하고 있습니다. 끊임없이 증가하는 사이버 범죄에 대처할 수 있도록 Google의 전문 지식을 공유하고 사회에 힘을 보태고 있으며Z, 모두에게 더 안전한 세상 을 만들기 위해 지속해서 최첨단 사이버 보안을 발전시키고 있습니다.



시대를 초월한 지속적인 혁신

Google은 2004년 Gmail을 출시한 이후 2022년 프로텍티드 컴퓨팅을 소개하기까지, 사이버 보안 기술을 개척하고 제품, 플랫폼, 그리고 파트너십을 지속적으로 혁신하여 이용자, 조직 및 사회를 위한 안전한 미래를 만들고자 모든 등급의 위협 요소를 제거하고 있습니다.

- ✓ 안전한 제품 및 플랫폼 개발
- ✓ 신속한 보안팀 구성
- ✓ 프로그램 및 파트너십 조성
- ✓ 혁신 및 인재 교육을 위한 자금 지원

사람들의 니즈와 인터넷 진화에 따라 시시각각 변화하는 사이버 위협을 줄이기 위해 새로운 기술을 선도하여 Google과 함께하는 매일이 더 안전하도록 노력합니다.

2004
Gmail 스팸 차단

Google은 AI 기반의 이메일 보호 기능을 구축한 최초의 기업 중 하나였습니다.

Gmail, 99.9%의 위험하고 의심스러운 이메일 차단

2007
세이프 브라우징

위험한 웹사이트에 방문 시 이를 이용자에게 경고하여 전 세계의 기기를 사전에 보호하였으며 2020년에는 이 온라인 보호 기능을 강화된 세이프 브라우징으로 발전시켰습니다.

세이프 브라우징 50억 개의 기기 보호

2009
reCAPTCHA

크리덴셜 스터핑 및 계정 탈취를 막고 악성 소프트웨어/가짜 이용자의 악의적 행위를 방지하기 위해 사기 및 봇 관리 솔루션을 확보했습니다.

500만 개의 웹사이트 방어

2008
Google 비밀번호 관리자

비밀번호 관리자의 도입으로 비밀번호를 외우거나 입력하지 않고도 쉽고 안전하게 로그인할 수 있게 되었으며 현재 모든 플랫폼의 50%에서 Chrome 로그인 기능을 사용하고 있습니다.

매일 10억 개의 비밀번호 위반 여부 확인

2010
제로 트러스트

Google은 수차례의 조직적인 사이버 공격, 오로라 작전을 거친 이후 현재는 '제로 트러스트'로 유명하며 기본적으로 안전한 아키텍처를 구축하는 접근 방식을 혁신했습니다. 이는 공격 벡터 감소, 데이터 손실 가능성 감소 및 이용자가 의존하는 시스템에 대한 제어를 강화합니다. Google은 미국 연방정부에 제로 트러스트 모델을 배포하고자 하는 백악관의 노력을 지지하며 모든 기업에서 이를 활용할 수 있도록 BeyondCorp Enterprise에 패키징했습니다.

2010
위협분석그룹(TAG)

오로라 작전 이후로 정부의 지원을 받는 심각한 범죄 사이버 위협 요소를 탐지, 분석 및 차단하는 일을 담당하는 전문팀을 구성했습니다. TAG는 사상 최대 규모의 랜섬웨어 공격인 워너크라이를 북한까지 추적했으며 최근에 인도, 러시아, 아랍에미리트 등에서 활동하는 고용 해커(hack-for-hire) 생태계 사례를 공유했습니다.

2010
Google 버그 헌터

Google의 취약성 보상 프로그램은 고등학생, 변호사, IT 전문가, 애호가를 대상으로 상금을 제시, Google 제품의 버그를 찾아냅니다. 참가자들의 동기는 다양하지만, 발견되지 않은 취약점을 찾아 온라인 서비스를 안전하게 보호한다는 사명만큼은 동일합니다.

2010년 이래로 수백만 달러의 상금 지급

2010
레드팀

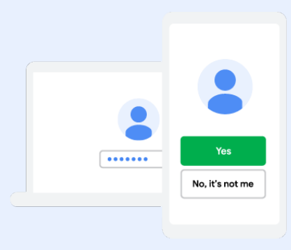
Google의 방어를 강화하고 빈틈을 발견하기 위해 Google에 대항하고 해킹하는 팀을 만들었습니다. 현시점의 위협 요소에 대응하고 보안 제어를 개선하며, 공격 탐지/예방을 수행하고, 새롭고 더 나은 프레임워크를 만들어 모든 등급의 취약점을 제거하고자 전 세계적으로 활동하고 있습니다.

2013
프로젝트 실드

프로젝트 실드는 위협 요소를 식별하고 보안 커뮤니티 및 법 집행기관에서 이에 대응 기능을 제공하여 사이버 공격이 발생하는 100여 개국의 뉴스, 인권 단체, 선거 사이트, 정치 단체 및 캠페인을 DDoS(Distributed Denial of Service) 공격으로부터 보호합니다.

현재 우크라이나에서 150개 이상의 웹사이트 보호

2011
2단계 인증



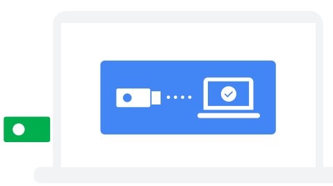
Google은 기본적으로 2단계 인증(2SV)을 제공하는 최초의 기업 중 하나였으며, 2021년에는 2SV를 자동으로 활성화하여 1억 5천만여 명에게 안전하고 쉬운 로그인 방식을 제공했습니다. 비밀번호를 도용당했더라도 계정은 보호됩니다.

2SV 이후 보안에 취약한 계정 50% 감소

2014
프로젝트 제로

안전하고 개방된 인터넷을 위해 소프트웨어, 하드웨어, Google 제품 등에서 인터넷의 제로데이 악용을 집중 추적하는 특별 태스크포스입니다. 'Meltdown'과 'Specter'를 처음으로 상세히 알려, 개발자들이 CPU 취약점을 신속히 해결하고 소프트웨어 공급망에 완화 조치를 하도록 하였습니다.

2017
고급 보호 프로그램 (APP)



언론인 및 국가 공무원처럼 가시성이 높은 고위험 이용자를 위해 보안 키를 포함하는 부가적인 보안 보호 기능입니다.

300개 이상의 연방 캠페인 보호

2018
Titan 보안 키

엔드 투 엔드 Google 솔루션을 원하는 이용자를 위해 Titan 보안 키를 개발했습니다. 이 키는 FIDO와 호환되며 Google뿐만 아니라 다른 사이트에서도 사용할 수 있습니다.

2019
비밀번호 없는 재인증

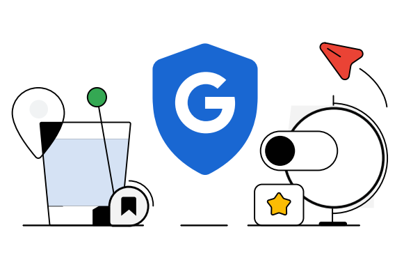
Android에서 FIDO 지원을 확장하여 이용자가 비밀번호 없이 PIN 또는 생체 인식만으로 웹사이트에 원활하게 로그인할 수 있습니다.

2017
Google Play 프로텍트

세계에서 가장 많이 배포된 모바일 위협 보호 서비스로 Google의 머신러닝을 사용하여 지속적으로 조정 및 개선하는 Google Play 프로텍트는 앱에서 자동으로 멀웨어를 스캔하고 Android 휴대전화에서 이용자 결제를 암호화합니다.

1,000억 개 이상의 이용자 매일 멀웨어 스캔

1억 5천만 명의 이용자 결제를 매일 암호화



2019
Chronicle

Chronicle은 핵심 인프라를 기반으로 하는 특수 레이어입니다. 기업에서 방대한 보안 및 네트워크 데이터를 비공개로 유지, 분석, 검색할 수 있도록 설계되어 클라우드 기반의 보안 서비스를 제공하기 위해 도입되었습니다.

2021
사이버 보안 강화에 투자

사이버 보안을 강화하고, 제로 트러스트 프로그램을 확장하며, 소프트웨어 공급망 보안 지원 및 오픈소스 보안 강화에 최선을 다합니다. Google 전문 수료증 과정을 통해 IT 지원 및 데이터 애널리틱스와 같은 분야에 있는 미국인 100,000명을 교육하기로 했습니다.

사이버 보안 이니셔티브에 미화 100억 달러 투자

2021
컨피덴셜 컴퓨팅

Google은 중요한 보안, 안전 및 개인정보보호를 위해 데이터가 처리되는 동안 데이터를 암호화된 상태로 유지하는 혁신적인 기술인 Google 클라우드 컨피덴셜 컴퓨팅을 도입하여 데이터를 저장 또는 전송 중일 때를 포함하여 전체 수명 주기 안에서 안전하게 유지할 수 있도록 합니다. 이제는 가장 민감한 데이터도 안심하고 클라우드로 마이그레이션할 수 있습니다.

2021
GOSST(Google 오픈소스 보안팀)

GOSST는 전 세계가 신뢰하는 오픈소스 소프트웨어의 보안을 개선하기 위해 마련되었습니다. OpenSSF(오픈소스 보안 재단)와의 협력으로 소프트웨어 공급망을 보호하고 장기적인 전체 소프트웨어 생태계 보안을 가능하게 하는 프레임워크인 SLSA(소프트웨어 아티팩트용 공급망 레벨)를 개발 및 공개했습니다.

취약점을 고치기 위해 타사 오픈소스 보안 운영에 미화 1억 달러 투자

2022
양자내성암호 표준화

Google은 공개키 암호화 파괴와 디지털 통신 손상을 보호하는 미래지향적인 차세대 암호화 시스템을 지속적으로 개발합니다.
미국표준기술연구소는 표준화를 위해 Google이 참여한 제출물(SPHINCS+)을 채택했습니다.

2022
프로텍티드 컴퓨팅

이용자의 개인정보보호와 안전을 기술적으로 보호하기 위해 데이터가 처리되는 방법, 시기, 위치를 혁신한 성장형 기술 툴킷인 프로텍티드 컴퓨팅을 발표했습니다. 데이터 저장 공간을 최소화하고, 데이터를 익명화하며, 민감한 데이터로의 액세스를 제한하는 방식으로 작동합니다. 즉, Android를 통해 대화를 완전히 비공개로 보호하면서 텍스트의 다음 문구를 제안할 수 있습니다.

2023
암호 없는 미래형 패스키

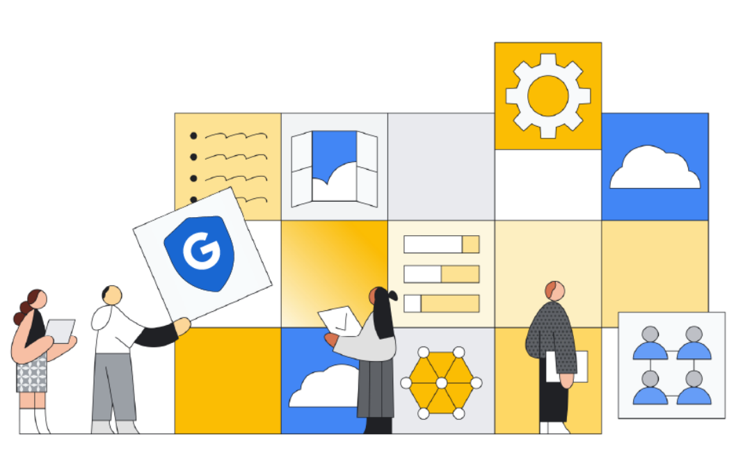
Google은 10년 넘게 비밀번호 없는 미래를 위한 기틀을 다져왔습니다. 년에 FIDO Alliance에 가입하여 비밀번호 없는 세상을 위해 개방형 표준을 추진하고 있으며 2023년 현재는 패스키 기술을 통해 Android 및 Chrome으로 FIDO 로그인 표준 지원을 확장하여 마침내 진정한 비밀번호 없는 미래를 위한 플랫폼을 선보이고자 합니다.

2022
Mandiant와 Google 클라우드

Mandiant는 거대 규모의 조직과 함께 사이버 보안의 최전선에서 확보한 심층적 실시간 위협 인텔리전스를 제공합니다. Google 클라우드의 클라우드 네이티브 보안 제품과 결합하여 기업 및 공공 부문 기관에서 보안 수명 주기 내내 보호할 수 있도록 합니다.

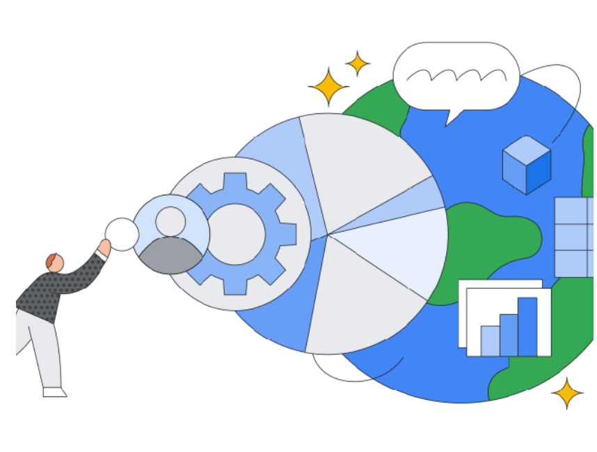
기술에 대한 신뢰는 끝없이 펼쳐지는 기술의 시대에 이 사회가 가진 진정한 잠재력을 여는 열쇠가 됩니다.

Google은 자사가 보유한 보안 지식을 실천하는 동시에 이용자, 기업 및 정부와 지속적으로 협력하여 안전을 지키고 사이버 보안의 새 시대를 주도할 것입니다.



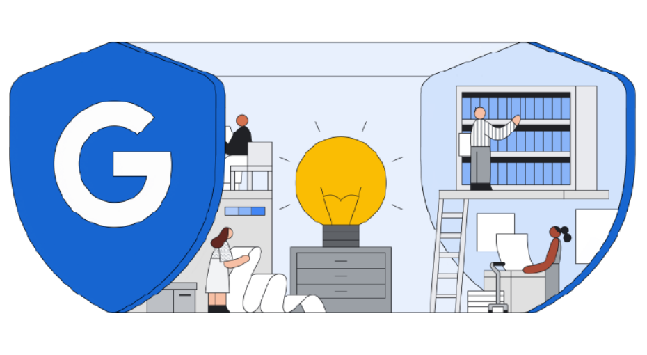
이용자, 기업 및 정부 보호

보안은 제품 전략의 핵심입니다.
그래서 Google의 모든 제품에는 보안을 제공하는 보호 기능이 기본적으로 내장되어 있습니다.



진화하는 사이버 보안 위험을 해결하기 위한 사회적 지원

오픈소스의 잠재력을 발휘할 수 있도록 사회에 힘을 보태고 Google의 지식 및 전문성을 업계와 투명하게 공유하여 더욱 안전하게 생태계를 보호합니다.



선도적인 미래 기술

사회를 차세대 사이버 위협 요소로부터 보호하고자 합니다.
AI 전문 지식을 기반으로 보안 혁신의 한계를 뛰어넘는 차세대 아키텍처를 설계하고 있습니다.

오늘도 Google과 함께라면 안전합니다

g.co/safety/cyber
방문하기

Google