# 모바일, 앱 및 IoT 보안

## 전 세계 데이터 및 기기 보호

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 있으며, 모두에게 더 안전한 세상을 만들기 위해 지속해서 최첨단 사이버 보안을 발전시키고 있습니다.

따라서 계속 증가하고 있는 위협 환경에 대처하려면 업계를 선도하며 보안 솔루션을 지속적으로 발전시키는 것이 중요합니다. 특히 커넥티드 기기 및 앱 보호 측면에서 소비자가 기기를 사용할 때 중개나 선택이 이루어지기 때문에 더욱 안전한 환경을 제공해야 합니다.

## 당면 과제

### 연결에는 대가가 따릅니다

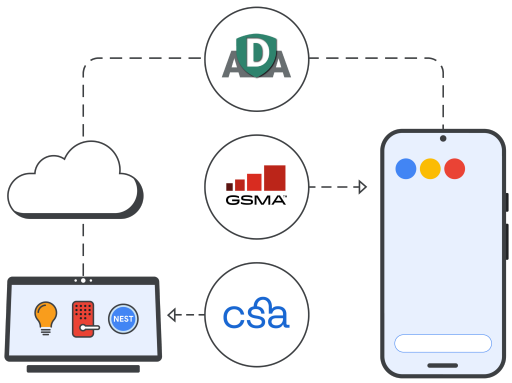
이용자들은 스마트폰, 앱 및 IoT 기기를 통해 갈수록 더 많은 시간을 온라인상에서 보내며, 그 과정에서 은행이나 의료 정보 등 중요한 데이터를 공유하며 일상을 보내고 있습니다. 그래서 최근 교활한 사이버 범죄자들이 이러한 기기를 범죄 대상으로 삼아 민감한 정보를 탈취하고 있습니다.

### 더 많은 기기, 더 많은 데이터는 더 많은 위협으로 이어집니다

프린터부터 차고 개폐기까지, 현재 전 세계적으로 약 170억 개의 IoT 기기가 존재하며 각 기기는 해킹하기 쉬운 소프트웨어(일부 오픈소스)를 사용하고 있습니다.[1] 전체적으로 보았을 때, 피해를 입은 IoT 기기의 수는 2020년 한 해 동안 거의 두 배로 증가했습니다.[2]

- 이용자들은 IoT 기기를 통해 점점 더 깊게 연결되고 있지만 연결된 제품의 보안 품질을 측정하는 글로벌 표준이 마련되어 있지 않기에 소비자는 기기 보안과 관련한 결정을 내릴 때 판단이 어려울 수 있습니다.
- 소비자에게는 직접 구매하는 식품이나 청소용품에 함유된 성분을 알 권리가 있듯이 디지털 제품의 투명성에 대한 알 권리 또한 주어져야 합니다.
- 모바일 기기는 수많은 공격 표면 중 하나의 벡터(공격 진입 경로)일 뿐이며, 기기의 상호 연결성은 대규모 보안 투명성에 대한 필요성을 증가시킵니다. 그러므로 커넥티드 기기 생태계 보안은 네트워크 및 시스템 보안만큼이나 중요합니다.

### 산업 기관과의 협력




## Google의 해결 방법

Google은 모바일, 앱 및 IoT 보안을 통해 연결된 기기의 보안 및 투명성을 개선하고 있습니다.

### 모바일 보안

Google의 오픈소스 운영 체제인 Android는 레이어드 시큐리티 접근 방식을 활용하여 모바일 기기를 안전하게 보호합니다.

- 레이어드 시큐리티
  - 자체 검사 부팅, 롤백 보호 및 공장 초기화 보호 기능으로 안전한 최신 Android 버전을 유지합니다.
  - PIN 및 생체 인증으로 외부 액세스를 차단합니다.
  - '내 기기 찾기' 기능을 통해 기기의 위치를 확인하거나 도난 또는 분실한 경우에 데이터를 삭제할 수 있습니다.
- ID 및 비밀번호 보호
  - 보안 키로 사용하는 휴대전화와 비밀번호 관리자의 2단계 검증을 통해 Google 계정에 대한 외부 액세스를 차단합니다.
  - 보안 점검 및 고급 보호 옵션으로 기기를 안전하고 원활하게 실행하도록 합니다.
- 안티피싱 보호
  - Phone by Google 및 Messages by Google은 스캠 및 피싱 공격을 감지하고 방지하는 데 도움이 됩니다.
  - Google 세이프 브라우징을 통해 전 세계적으로 50억 개 이상의 기기를 보호합니다.

### 앱 보안

뛰어난 성능의 안티멀웨어로 악성 앱을 차단하고 데이터 보안 정보로 앱 다운로드 시 이용자에게 투명성을 제공합니다.

- Google Play 스토어: 모든 앱은 Google Play 스토어에 출시되기 전에 머신러닝 감지 도구 및 분석 전문가에게 검토받습니다. 데이터 보안 섹션을 통해 앱에서 수집하는 데이터 유형 및 해당 데이터 용도를 설명합니다.
- Google Play 프로텍트: 1,250억 개의 앱을 매일 스캔하고 보안 위험이 감지될 경우 알림, 제거 또는 비활성화합니다.
- ADA(App Defense Alliance): Google은 업계를 선도하는 모바일 위협 감지 파트너사와 협력하여 공유형 인텔리전스 및 공동 감지를 통해 Android 사용자를 PHA(잠재적으로 유해한 애플리케이션)로부터 보호하는 App Defense Alliance를 공개했습니다.

### IoT 보안

IoT 보안 레이블은 개인정보보호 및 보안 수칙에 따라 기기에서 어떤 개인정보가 수집되고 있는지 등을 확실하게 전달합니다.

- IoT 보안 레이블링 체계의 5가지 핵심 원칙으로는 실시간 레이블, 평가 체계, 유연성 관련 보안 기준, 광범위한 투명성, 인센티브 도입이 있습니다.
- 기존 및 향후 규제 요건에 대한 업계 전반의 인증 프로그램을 표준화하기 위해 CSA(Connectivity Standards Alliance) 및 GSMA(GSM Alliance)와 협력하고 있습니다.

## Google의 원칙

**Google은 커넥티드 기기의 보안 및 투명성을 개선하기 위해 3가지 핵심 원칙을 적용합니다**

심층 방어: 함께 작동하는 여러 계층의 보안 아키텍처를 활용하여 원활하며 효율적으로 실행되는 강력한 방어를 구축합니다.

개방성 및 투명성: 투명성은 Google 철학의 핵심입니다. 플랫폼 이용자 보호를 강화하기 위한 지속적인 정보 제공과 지식 공유를 통해 오픈소스 생태계는 폐쇄적인 생태계보다 더욱 안전할 수 있습니다.

Google 및 생태계의 장점: Google 내부의 전문가만이 아니라 업계 전문팀과 협력하여 수십억 명 이용자의 안전을 보호합니다.

## 애플리케이션

### 소비자에게 제어 권한을 부여하는 IoT 보안 레이블

확립된 IoT 보안 레이블링 외에는 기기 제조업체에서 준수해야 하는 글로벌 표준이 존재하지 않습니다. 이용자 또한 본인 소유 기기의 데이터 보호 여부를 파악하기 어렵습니다. IoT 보안을 촉진하고 소비자에게 제어 권한을 다시 부여하기 위해서는 업계가 서로 협력해야 합니다. Google은 프로세스 및 파트너십을 통한 IoT 보안 레이블링 체계를 지향하고 있습니다.

우선 잠재적 취약점을 찾아내고자 외부 보안 리서치에 투자합니다(Google Nest는 취약성 보상 프로그램 참여를 통해 취약점을 발견한 Google 외부 보안 연구원에게 보상을 제공하고 있습니다).

이후 이러한 취약점을 공개하고 최소 5년 동안 중요한 버그 패치 및 수정 사항을 공지합니다.

2019년 이후 개발된 모든 기기는 자체 검사 부팅을 사용해 알맞은 소프트웨어가 실행 중이고 액세스가 보호되고 있는지 확인합니다. 예를 들어, Google Nest 기기 는 NIST, ETSI, ISO 등 업계에서 인정하는 타사 보안 표준을 사용해 검증합니다.

이러한 표준과 Google의 안전한 SDLC(소프트웨어 개발 수명 주기)는 소비자가 열악한 보안 관행에 노출될 가능성을 줄이고 개방적이면서도 안전한 인터넷을 위한 기틀을 마련합니다.

## 업계 투자 및 주요 성과

**2007** 세이프 브라우징 확립
위험한 웹사이트 방문 시 이용자에게 사전 경고하며 현재 50억 개 이상의 기기를 보호하고 있습니다.

**2010** Google 투명성 보고서 공개
정부 및 기업의 정책 겸 조치가 개인정보보호, 보안 및 온라인 정보 액세스에 미치는 영향을 보여줍니다. 2018년, Google은 Android 특정 투명성 보고서를 추가했습니다.

**2017** Google Play 프로텍트 출시
가장 많이 배포된 안티멀웨어 솔루션으로, 현재 30억 대 이상의 기기에서 하루에 1,250억 개 이상의 앱을 스캔하고 있습니다.

**2019** 보안 키 도입
Android 기본 기능으로 제공되고 있으며 iPhone의 경우 2020년에 도입하였습니다.

**2022** Google Play 출시
앱에서 사용자 데이터를 수집, 공유 및 보호하는 방법에 대한 자세한 정보를 사람들에게 제공하는 데이터 보안 섹션입니다. App Defense Alliance를 통해 최초로 독립적인 보안 검토를 완료한 모든 앱에는 배지를 부여하는 시스템도 실시했습니다.

**2023** 비밀번호 없는 미래형 패스키
지난 10년 동안 FIDO Alliance 및 세계적인 테크 선두업체와 함께 개방형 표준을 주도하며 확장형 패스키 지원과 함께 활용되고 있습니다.

## Google의 접근 방식

### 개방적이고 안전한 디지털 환경을 위한 노력

보안 문제는 다양한 네트워크에 연결된 기기의 수와 데이터가 많아질수록 심각해집니다. Google은 제품 개발, 투명성 기준, 산업 파트너십을 통해 커넥티드 기기 보안의 미래를 개척하도록 지원합니다.

Google의 제품 전략은 기본적으로 제품의 안전성을 보장하는 것을 그 핵심으로 합니다. 세이프 브라우징, Google Play 프로텍트, 내장 보안 키는 제품에 강력한 보안을 제공하여 모바일 기기 및 앱을 보호합니다.

개방적이며 투명하게 문제를 해결하고 커넥티드 기기 보안 지식을 공유함으로써 보안 운영의 민주화를 지원합니다. 오픈소스 생태계가 레이어드 시큐리티 접근 방식의 폐쇄적인 생태계보다 더욱 안전할 수 있을 것이라고 믿습니다.

CSA, ADA, GSMA 내에서의 협력을 통해, 모두를 위한 더 안전한 인터넷과 미래 사이버 보안의 최첨단 기술을 개선하고자 매진하고 있습니다.

커넥티드 기기 보안의 기준을 높이고 누구든지 어디서나 이용할 수 있는 더 안전한 온라인 환경에 대한 표준을 설정하고자 최선을 다하고 있습니다. 커넥티드 기기 보안의 Google 프로세스는 g.co/connecteddevicesafety 에서 자세히 알아보세요

출처: [1] 2023년 1월 9일 CNBC Cyber Report, [2] 2021년 7월 20일 What is an IoT Attack? The Ins and Outs of IoT Security