Seguridad de apps, dispositivos móviles y del IoT

Cómo protegemos los datos y los dispositivos en el mundo

Considerando el incremento radical de los ciberataques patrocinados por gobiernos y actores maliciosos en línea, creemos que nuestros productos y servicios son tan útiles como seguros. En Google, estamos más enfocados que nunca en proteger a las personas, las organizaciones y los gobiernos con nuestra experiencia: capacitamos la sociedad para combatir los riesgos cibernéticos en constante evolución y trabajamos continuamente para progresar en el arte de la ciberseguridad para construir un mundo más seguro para todas las personas.

Como tal, es imperativo mantenernos a la vanguardia y mejorar constantemente nuestras soluciones de seguridad para combatir el panorama de amenazas en constante crecimiento, en particular cuando se trata de proteger los dispositivos y las apps conectados. Al hacerlo, ofrecemos a los consumidores un entorno seguro para tomar decisiones sobre los dispositivos que utilizan.

El reto

La conectividad tiene un precio

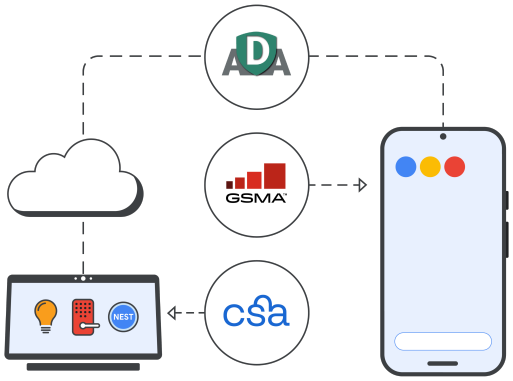
Gran parte de nuestra vida cotidiana es gestionada desde nuestros smartphones, apps y dispositivos contectados al Internet de las cosas (IoT). Cada vez pasamos más tiempo en línea y compartimos datos valiosos, como información bancaria o médica, en el proceso. Debido a esto, los ciberdelincuentes astutos se enfocan más que nunca en atacar estos dispositivos para obtener información confidencial.

Más dispositivos, más datos, más amenazas

En la actualidad se calcula que hay 17,000 millones de dispositivos conectados al IoT en el mundo, desde impresoras hasta puertas de garaje, cada uno repleto de software (algunos de código abierto) que pueden ser fácilmente pirateados.[1] En total, el número de dispositivos IoT en peligro casi se duplicó en 2020.[2]

- Aunque los dispositivos IoT nos mantienen cada vez más en contacto, no existen normas mundiales para medir la calidad de la seguridad de los productos conectados, así que los consumidores no tienen información para tomar decisiones sobre la seguridad de los dispositivos.
- Los consumidores deben tener derecho a la transparencia sobre sus productos digitales, así como tienen derecho a saber qué ingredientes hay en los alimentos o en los productos de limpieza que compran.
- Los dispositivos móviles son solo un segmento de las superficies de ataque, y la interconectividad de los dispositivos aumenta la necesidad de transparencia de la seguridad a escala. Por este motivo, la seguridad del ecosistema de dispositivos conectados es tan importante como la de las redes y los sistemas.

Colaboramos con organizaciones del sector



Nuestra solución

En Google, mejoramos la seguridad y la transparencia de nuestros dispositivos conectados a través de la seguridad para móviles, apps y el IoT:

Seguridad para móviles

Android, nuestro sistema operativo de código abierto, utiliza un enfoque de seguridad por capas para mantener seguros los dispositivos móviles:

- Seguridad por capas
  - El inicio verificado, la protección retroactiva y la protección en el restablecimiento de la configuración de fábrica, garantizan la versión más reciente y segura de Android.
  - El PIN y la autenticación biométrica protegen contra el acceso externo
  - La función “Encontrar mi dispositivo” sirve para localizar dispositivos o para borrar su contenido en caso de robo o pérdida.
- Protección de identidad y contraseña
  - La Verificación en dos pasos, la Llave de seguridad integrada del teléfono y el Administrador de contraseñas protegen tu cuenta de Google contra el acceso externo.
  - La Verificación de seguridad y la Protección Avanzada opcional mantienen el dispositivo funcionando de forma segura y sin problemas.
- Protección contra la suplantación de identidad (phishing)
  - Las apps Teléfono de Google y Mensajes de Google ayudan a detectar y prevenir ataques de estafa y suplantación de identidad.
  - Google Safe Browsing protege más de 5,000 millones de dispositivos en todo el mundo.

Seguridad para apps

El antimalware integrado ayuda a mantener alejadas las apps maliciosas y la información sobre la seguridad de los datos proporciona transparencia a los usuarios al descargar apps.

- Google Play Store: Las herramientas de aprendizaje automático enfocadas en detección y las personas analistas revisan todas las apps antes de que estén disponibles para su descarga. La sección Seguridad de datos explica qué tipo de datos recopilan las aplicaciones y para qué son utilizados.
- Google Play Protect: Analiza más de 125,000 millones de apps cada día y notifica, las elimina o desactiva si se detectan riesgos para la seguridad.
- App Defense Alliance (ADA): Google trabajó con los principales socios de detección de amenazas móviles para lanzar App Defense Alliance, que utiliza inteligencia compartida y detección coordinada para proteger a los/las usuarios/as de Android de las aplicaciones potencialmente dañinas.

Seguridad del IoT

Las etiquetas de seguridad del IoT divulgan claramente las prácticas de privacidad y seguridad en un dispositivo, como los datos recopilados.

- Creemos en cinco principios básicos para los esquemas de etiquetado de seguridad del IoT: etiquetado en tiempo real, sistemas de evaluación, líneas básicas de seguridad combinadas con flexibilidad, amplia transparencia e incentivos de adopción.
- Estamos trabajando con Connectivity Standards Alliance (CSA) y GSM Alliance (GSMA) para estandarizar un programa de certificación que sirva a todo el sector para cumplir los requisitos regulatorios actuales y futuros.

Nuestros principios

En Google, aplicamos 3 principios básicos para potenciar la seguridad y la transparencia de nuestros dispositivos conectados:

Defensa en profundidad Utilizamos múltiples capas arquitectónicas de seguridad que trabajan en conjunto para crear una defensa sólida que funcione sin problemas y con eficacia.

Apertura y transparencia La transparencia es la clave de nuestra filosofía. Mantenemos informados/as a los/las usuarios/as de nuestra plataforma y compartimos conocimientos para reforzar nuestra protección, porque creemos que un ecosistema de código abierto puede ser más seguro que uno cerrado.

Lo mejor de Google y de nuestro ecosistema Colaboramos con equipos de expertos de Google y del sector para mantener la seguridad de miles de millones de usuarios/as.

Aplicaciones

Con las etiquetas de seguridad del IoT, los consumidores tienen el control

Si no existe un etiquetado de seguridad para el IoT, no existen normas globales para los fabricantes de dispositivos. Los usuarios tampoco tienen la visibilidad que merecen sobre si sus dispositivos protegen sus datos. La industria debe unirse para impulsar la seguridad del IoT y devolver el control a los consumidores. Estamos trabajando con nuestros procesos y asociaciones para crear un sistema de etiquetado de seguridad del IoT.

En primer lugar, invertimos en investigación de seguridad externa para detectar posibles vulnerabilidades (Google Nest participa en el programa de recompensas por vulnerabilidades de Google y ofrece recompensas a los investigadores de seguridad externos a Google que encuentren vulnerabilidades).
Luego, publicamos parches y correcciones de errores críticos durante mínimo cinco años después del lanzamiento.
Todos nuestros dispositivos desarrollados a partir de 2019 utilizan el Inicio verificado para garantizar que se ejecuta el software correcto y que el acceso está protegido. Por ejemplo, nuestros dispositivos Google Nest se validan utilizando estándares de seguridad de terceros reconocidos por la industria, como los desarrollados por NIST, ETSI e ISO.

Estos estándares, y nuestro Ciclo de Vida de Desarrollo de Software Seguro (SDLC), reducen la probabilidad de que las/los consumidoras/es se vean expuestos a malas prácticas de seguridad y preparan el camino hacia un internet abierto y más seguro.

Nuestras inversiones y logros en la industria

2007 Creación de Navegación segura para alertar de forma proactiva a los usuarios cuando visitan sitios web peligrosos. Ya protege a más de 5,000 millones de dispositivos.

2010 Lanzamiento del Informe de transparencia de Google para mostrar cómo las políticas y acciones de los gobiernos y las empresas afectan la privacidad, la seguridad y el acceso a la información en línea. En 2018 creamos un Informe de transparencia específico para Android.

2017 Lanzamiento de Google Play Protect, que ahora es la solución antimalware más extendida: escanea más de 125,000 millones de apps al día en más de 3,000 millones de dispositivos.

2019 La Llave de seguridad se presentó como una función integrada en Android y luego para iPhone en 2020.

2022 Google Play lanzó una sección de seguridad de datos para ofrecer a las personas más información sobre cómo las aplicaciones recopilan, comparten y protegen los datos de las/los usuarias/os, e inició el primer sistema de distintivos para cualquier aplicación que haya completado una revisión de seguridad independiente a través de la App Defense Alliance (Alianza para la defensa de las aplicaciones).

2023 Llave de acceso: un futuro sin contraseñas se pone en marcha con la ampliación de la compatibilidad con Llave de acceso tras una década impulsando estándares abiertos con la Alianza FIDO y líderes tecnológicos de todo el mundo.

Nuestro enfoque

Comprometidos con un mundo digital abierto y seguro

La preocupación por la seguridad no hará más que aumentar debido al incremento de datos en más dispositivos y a través de diferentes redes. Queremos mejorar el futuro de la seguridad de los dispositivos conectados a través del desarrollo de nuestros productos, criterios de transparencia y alianzas en la industria.

Una piedra angular de nuestra estrategia de producto es garantizar que nuestros productos sean seguros por diseño. La Navegación segura, Google Play Protect y las Llaves de seguridad integradas protegen los dispositivos móviles y las aplicaciones para ofrecer el máximo nivel de seguridad en nuestros productos.

Buscamos democratizar las operaciones de seguridad siendo abiertos y transparentes en la forma de abordar los problemas y compartiendo información de seguridad sobre los dispositivos conectados. Creemos que un ecosistema de código abierto puede ser más seguro que un ecosistema cerrado gracias a nuestro enfoque de seguridad por capas.

Al colaborar con CSA, ADA y GSMA buscamos progresar en el arte de la ciberseguridad para construir un internet y un futuro más seguro para todos.

Nos comprometemos a elevar el estándar de seguridad de los dispositivos conectados y a crear un entorno online más seguro para todos y todas y en todas partes. Más información sobre los avances de Google en la seguridad de los dispositivos conectados: g.co/connecteddevicesafety

Fuentes: [1] CNBC Cyber Report, 9 de enero de 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, 20 julio de 2021