

Defensa contra amenazas móviles en Android, iOS y Chromebook

Los smartphones y las tablets son dispositivos móviles que han transformado nuestra forma de conectarnos y trabajar. De hecho, tanto los empleados como las empresas dependen cada vez más de estos dispositivos. No obstante, el hecho de que los empleados accedan a canales de comunicación como el correo electrónico, los SMS, el chat y las apps ha promovido la aparición de nuevos riesgos en los lugares de trabajo. Muchos empleados acceden ahora a los datos (listas de clientes, detalles bancarios, datos personales de la plantilla laboral, información de facturación, etc.) y sistemas corporativos (mensajes, herramientas de colaboración, ERP, etc.) desde sus dispositivos móviles como lo harían desde una mesa en la oficina. Esto implica que el compromiso de un dispositivo móvil puede ahora suponer un riesgo notable para los datos de los clientes, la propiedad intelectual y los sistemas centrales.

¿Por qué necesitan protección los dispositivos móviles?

→ El correo electrónico sigue siendo el principal medio de los ataques de phishing (90 %) y un 60 % de los mensajes de correo electrónico se abren en dispositivos móviles (informe sobre investigaciones de violaciones de la seguridad de Verizon 2022).

→ El 18 % de los correos electrónicos de phishing en los que se hizo clic se abrieron desde un dispositivo móvil (informe sobre investigaciones de violaciones de la seguridad de Verizon 2022).

→ El 79 % de la gente admitió usar dispositivos del trabajo para tareas personales, como consultar el correo electrónico personal, hacer compras o ver vídeos en streaming (informe sobre investigaciones de violaciones de la seguridad de Verizon 2022).

Según Gartner®, “los productos de defensa contra amenazas móviles (MTD) utilizan diversas técnicas, como por ejemplo el análisis del comportamiento, para contrarrestar las amenazas en estos dispositivos. Los proveedores de plataformas de protección de endpoints (EPP) siguen reforzando sus ofertas y poniéndose al día con funcionalidades de proveedores de MTD independientes”.¹

GravityZone Security para dispositivos móviles protege los dispositivos móviles para que los empleados puedan acceder con seguridad a los datos corporativos. Detecta tanto amenazas conocidas como desconocidas, incluidos ataques de día cero, de phishing y de red. En cuanto se implementa en un dispositivo móvil, empieza a protegerlo contra los principales vectores de ataque, incluso aunque el dispositivo no esté conectado a una red.

GravityZone Security para dispositivos móviles protege contra los modernos vectores de ataque tanto los dispositivos propiedad de la empresa como los que traen los propios empleados. Se ha diseñado teniendo en cuenta la privacidad empresarial y personal y ofrece lo siguiente:

→ Seguridad y privacidad de los dispositivos móviles. Seguridad informática de alta calidad en apps, tráfico web y dispositivos. Amplio abanico de puntos de detección para proporcionar un control más granular de las políticas de cumplimiento.

→ Seguridad independiente de la plataforma y del dispositivo. Cubre las tres plataformas principales: iOS, Android y Chrome OS.

→ Minimización de riesgos. Detecta vulnerabilidades de dispositivos móviles y

En resumen

GravityZone Security para dispositivos móviles es la herramienta de seguridad integral que aborda las amenazas para los dispositivos móviles con el fin de ayudar a las organizaciones a conseguir lo siguiente:

→ Entender su huella móvil.

→ Obtener visibilidad y valiosa información sobre los riesgos asociados a los dispositivos móviles.

→ Proteger y prevenir los ataques contra dispositivos móviles.

→ Detectar y responder ante dispositivos comprometidos.

→ Integrar los datos móviles en los informes generales sobre la seguridad.

Principales beneficios

GravityZone Security para dispositivos móviles contribuye a todo lo anterior con el cumplimiento normativo y la habilitación del modelo de confianza cero para el acceso a la red desde dispositivos móviles, ya que:

→ Proporciona protección y visibilidad de las amenazas para los dispositivos móviles.

→ Reduce el riesgo de robo de datos y pérdida de credenciales.

→ Favorece el cumplimiento normativo con la detección de aplicaciones que incumplan y el mantenimiento de un catálogo de aplicaciones permitidas.

→ Minimiza el incumplimiento del RGPD al limitar la recopilación de datos de dispositivos personales.

→ Admite tanto trabajo remoto como híbrido.

¹ Gartner, Guía del mercado de defensa contra amenazas móviles, 10 de enero de 2023

acciones o configuraciones que incumplen las normativas.

→ Una sola consola para todo lo relacionado con la seguridad. Se integra con GravityZone para brindar una visibilidad y seguridad de extremo a extremo en todas las plataformas.

Características clave

GravityZone Security para dispositivos móviles brinda protección integral para dispositivos móviles.

Protección de aplicaciones

→ Aprovecha las tecnologías de Machine Learning tanto dentro como fuera del dispositivo para detectar app maliciosas (iOS y Android).

→ Detección de aplicaciones que incumplen las normativas (evaluación de aplicaciones).

Protección Web

→ Antiphishing en dispositivos móviles.

→ Control de acceso Web.

Protección de red

→ Detección de amenazas transmitidas por la red, intentos de reconocimiento, conexiones de escasa seguridad y ataques man-in-the-middle.

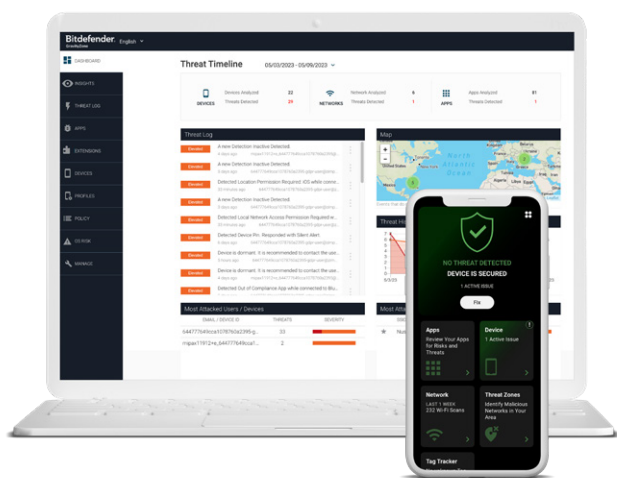
Protección de dispositivos

→ Detección de vulnerabilidades del sistema operativo, dispositivos vulnerables que no pueden actualizarse, etc.

→ Detección de falta de cifrado, jailbreak o root, manipulación del sistema, etc.

GravityZone Cloud MSP Security para dispositivos móviles

GravityZone Cloud MSP Security para dispositivos móviles brinda a los proveedores de servicios administrados (MSP) las herramientas que precisan para proteger los dispositivos móviles ante posibles amenazas. Los MSP pueden garantizar que sus datos y redes permanecen a salvo así como la protección de la información de sus clientes. Esta completa solución de defensa contra amenazas móviles (MTD) cuenta con una única consola multiusuario fácil de usar y un flexible sistema de licencias basado en el uso mensual.



Gartner® es una marca registrada y una marca de servicio de Gartner, Inc. y/o sus filiales en los Estados Unidos e internacionalmente. Se mencionan aquí con autorización. Todos los derechos reservados.

Bitdefender es uno de los líderes mundiales en seguridad informática que protege más de 500 millones de sistemas en más de 150 países. Desde 2001, la innovación de Bitdefender ha lanzado de manera sistemática productos de seguridad galardonados e inteligencia sobre amenazas para hogares conectados e inteligentes, usuarios de dispositivos móviles, empresas modernas y sus redes, dispositivos, centros de datos e infraestructuras de nube. Actualmente, Bitdefender es también el proveedor de seguridad preferido, integrado en más del 38 % de las soluciones de seguridad del mundo. Reconocida por el sector, respetada por los proveedores y recomendada por los clientes, Bitdefender es la empresa de seguridad informática en la que puede depositar su confianza.

Todos los nombres de productos y empresas mencionados en este documento se citan con una finalidad meramente identificativa y podrían pertenecer o ser marcas comerciales de sus respectivos propietarios.