MOTOTRBO ION

SEGURIDAD EN ACCION

MOTOTRBO Ion le ayuda a mantenerse seguro de las amenazas cibernéticas. Nuestro acercamiento de defensa profunda le proporciona varias capas de seguridad para ayudarle a prevenir el acceso de dispositivos no autorizados y la actividad mal intencionada, y a salvaguardar sus datos críticos. Al contar con el máximo nivel de seguridad en dispositivos y redes, en combinación con un monitoreo de amenazas en tiempo real, Ion le permite utilizar datos y aplicaciones de Android con confianza; aún en las redes privadas.

SEGURIDAD DE DISPOSITIVO PARA PREVENIR EL ACCESO NO AUTORIZADO

MOTOTRBO ION AYUDA A PREVENIR QUE EL CÓDIGO HOSTIL SE EJECUTE EN EL DISPOSITIVO PARA QUE LOS USUARIOS NO AUTORIZADOS NO OBTEGAN ACCESO.

AMBIENTE DE EJECUCIÓN CONFIABLE (TEE)

Un TEE proporciona seguridad de extremo a extremo implementando la tecnología TrustZone de ARM así como funciones y servicios críticos de manos libres. Se ejecuta en el mismo procesador que el sistema operativo de Android, pero se encuentra completamente aislado del resto del sistema. El aislamiento garantiza que los datos críticos se almacenen, procesen y protejan en un ambiente seguro.

FIRMWARE CONFIABLE

Un proceso de arranque seguro verifica la integridad tanto del firmware como del software. Con secure boot, cada etapa del proceso de arranque se firma criptográficamente con claves aprobadas, lo cual previene los ataques mal intencionados y las actualizaciones de software no autorizadas, proporcionando un lanzamiento seguro y confiable.

EL SISTEMA ANDROID KEYSTORE

Android Keystore previene el uso no autorizado de claves criptográficas. Adicionalmente, las apps deben especificar los usos autorizados de sus claves y requerir que se utilicen estas restricciones fuera de los procesos de las mismas, proporcionando aún más restricciones en cómo y cuándo se utilizan dichas claves.

SEGURIDAD DE ACCESO A DISPOSITIVOS

MOTOTRBO Ion tiene compatibilidad con mecanismos de factor sencillo y múltiple; desde PIN sencillo hasta otros factores de autenticación tales como contraseñas, patrones, etc. Los usuarios válidos tendrán acceso solo a los datos, aplicaciones y servicios para los cuales se han autorizado.

EL MARCO DE TRABAJO DE CIBERSEGURIDAD DEL NIST

Todos los sistemas y dispositivos MOTOTRBO se apegan estrictamente al marco de trabajo de ciberseguridad del NIST.

Las prácticas de seguridad del NIST se basan en un monitoreo, diagnóstico, opciones de mitigación y corrección continuos. Utilizamos un acercamiento basado en riesgos a través de todo nuestro proceso en el ciclo de vida del desarrollo, implementación y soporte operativo. Nuestra protección y controles basados en respuestas se crean con la consulta de los principales expertos de la industria, los procesos y las tecnologías.

MOTOROLA SOLUTIONS

SEGURIDAD DE APLICACIONES PARA PREVENIR LA ACTIVIDAD MAL INTENCIONADA

MOTOTRBO ION HABILITA LA OPERACIÓN SEGURA AYUDANDO A PREVENIR EL MALWARE, PHISHING Y OTROS TIPOS DE ACTIVIDAD MAL INTENCIONADA.

ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES Y GOOGLE PLAY ADMINISTRADO

Las políticas de seguridad, incluyendo la administración de aplicaciones, se implementan mejor utilizando una solución de Administración de Dispositivos Móviles (MDM). Los administradores de TI, quienes habitualmente son responsables por la configuración y administración de estos dispositivos, pueden utilizar un MDM para definir y configurar las políticas para el uso de aplicaciones, lo cual crea un marco de trabajo de administración de aplicaciones a la medida de sus necesidades específicas.

Una clave para esta implementación es el marco de trabajo de Android Enterprise y de Google Play Administrado, los cuales proporcionan las API para los proveedores de MDM para administrar apps en dispositivos Android.

Esto aplica tanto a las aplicaciones públicas disponibles desde Google Play Store como a las aplicaciones privadas que se crean para uso

A través de la MDM, los administradores de TI pueden:

- Distribuir remotamente las aplicaciones aprobadas mediante la Google Play Store administrada y bloquear las aplicaciones mal intencionadas o borrarlas
- Definir y habilitar/inhabilitar el acceso para los usuarios dependiendo de su perfil
- Configurar notificaciones en tiempo real sobre el uso de dispositivos para monitorear la actividad mal intencionada o la falta de cumplimiento de las políticas de seguridad.

GOOGLE PLAY PROTECT

Google Play Protect es un poderoso servicio de detección de amenazas que se desarrolla dentro de la Google Play Store, el cual escanea activamente 24x7 en busca de aplicaciones dañinas y protege del malware a los dispositivos, sus datos y aplicaciones. Se notifica a los usuarios cuando se detecte alguna app que contenga malware. Google Play Protect también podría eliminar o inhabilitar las apps mal intencionadas automáticamente como parte de su iniciativa de prevención y utilizar la información que recaba para mejorar la detección de Aplicaciones Potencialmente Dañinas (PHA). Adicionalmente, el usuario también podría optar por que se envíen las aplicaciones desconocidas a Google para su análisis.

SAFETYNET

SafetyNet es un conjunto de API y servicios que pueden utilizar los desarrolladores para proteger las apps de las amenazas de seguridad y mitigarlas contra manipulación mal intencionada de dispositivos, URL malignas, PHA y usuarios falsos.

INGRESO A LAS APLICACIONES

Android requiere que todas las apps se firmen digitalmente con una clave de desarrollador antes de que se instalen y utiliza el certificado correspondiente para identificar al autor de la aplicación. Cuando el sistema instala una actualización para una aplicación compara el certificado en la nueva versión con aquella existente y solo permite dicha actualización si el certificado coincide.

SEGURIDAD DE DATOS PARA SALVAGUARDAR AQUELLOS CRÍTICOS

MOTOTRBO ION SALVAGUARDA LOS DATOS CRÍTICOS, TANTO ESTÁTICOS COMO EN TRÁNSITO.

SEGURIDAD DE DATOS ESTÁTICOS

ALMACENAMIENTO SEGURO

Las credenciales, los certificados y las claves se almacenan de forma segura en un área de almacenamiento respaldada por hardware en el dispositivo.

MANEJO DE CERTIFICADOS

Las autoridades de certificados son críticas para proporcionar comunicaciones seguras a través de una red utilizando la infraestructura de llave pública. Con Android 7.0 y superior, todos los dispositivos compatibles, incluyendo a MOTOTRBO Ion, implementarán únicamente las autoridades de certificados con sistemas estandarizados que se mantienen en el AOSP. Los dispositivos Ion se enviarán con el mismo almacén de autoridad de certificados.

PERFIL DE TRABAJO

Para los dispositivos que pertenezcan a la compañía, los administradores de TI pueden implementar una o dos opciones de despliegue para administrar los datos corporativos en estos dispositivos:

- Dispositivo completamente administrado en donde éste se utiliza exclusivamente para propósitos laborales. Los administradores de TI pueden requerir la gama completa de políticas administrativas para el dispositivo integral
- Opción de perfil de trabajo completamente administrada en donde el dispositivo es compatible con el perfil de trabajo y un perfil personal, simultáneamente

En la segunda opción, el perfil de trabajo crea un perfil separado y auto-contenido que contiene aplicaciones y datos corporativos, y que los aísla de las aplicaciones y datos personales. Al utilizar la MDM, pueden configurarse las políticas del dispositivo para prevenir que se compartan archivos y datos desde el perfil de trabajo.

POLÍTICAS DEL DISPOSITIVO

El dispositivo puede configurarse utilizando una MDM para prevenir o restringir la transferencia de datos desde/hacia el dispositivo, tal como:

- Prevenir la transferencia de archivos utilizando Bluetooh
- Prevenir la transferencia de archivos desde el dispositivo a través del USB
- Prevenir el acceso al almacenamiento externo, tal como una tarjeta SD
- Prevenir que se monten medios físicos externos
- No admitir el acceso a las capacidades de depuración
- Configurar las políticas del passcode del dispositivo
- Inhabilitar la cámara
- Inhabilitar la captura de pantalla
- Permitir la instalación de apps desde fuentes conocidas, tales como Google Play store

SEGURIDAD DE LOS DATOS EN TRÁNSITO

Ion implementa los protocolos seguros estándar de la industria que se utilizan para los datos en tránsito, tales como SRTP, HTTPS, etc. Se han implementado los protocolos estándar de la industria disponibles, así como los requisitos de seguridad para interfaces de conectividad tales como WiFi, USB, Bluetooth y VPN. Adicionalmente, Android proporciona comunicaciones seguras a través de Internet para las búsquedas web, el correo electrónico, la mensajería instantánea y otras aplicaciones de Internet, al ser compatible con la Seguridad de Capa de Transporte (TLS).

WI-FI

Android 10 es compatible con el acceso protegido de WiFi versión 3 (WPA3) de la alianza de Wi-Fi y con los estándares abiertos y ampliados de Wi-Fi, lo cual mejora la seguridad general al proporcionar una mejor privacidad y una robustez contra los ataques conocidos.

VPN

Android es compatible con el conectarse de forma segura a una red empresarial utilizando una VPN.

MEDIDAS DE SEGURIDAD ADICIONALES

ACTUALIZACIONES DE SEGURIDAD DE ANDROID

Cada mes, Google publica Boletines de Seguridad de Android para actualizar a los usuarios, socios y clientes sobre las últimas correcciones. Estas actualizaciones de seguridad se encuentran disponibles para las versiones de Android durante tres años desde la fecha de lanzamiento.

PROGRAMA DE ANDROID ENTERPRISE RECOMMENDED

El programa de Android Enterprise Recommended para Google proporciona un conjunto de especificaciones para los dispositivos empresariales y para los servicios de rendimiento de hardware, actualizaciones de seguridad y experiencia del usuario. Esto incluye las actualizaciones de seguridad que se entregan a los dispositivos en los primeros 90 días después de su lanzamiento en Google. Adicionalmente, las OEM reciben un nivel ampliado de soporte técnico y capacitación.

ESTÁNDARES DE LA INDUSTRIA Y CERTIFICACIONES

Android Enterprise ha recibido la certificación ISO 27001 y los reportes de SOC 2 y 3 por sus prácticas y procesos de seguridad informática de la API de Administración de Android, su inscripción sin intervención y por Google Play administrado. Esta designación garantiza que estos servicios cumplan con estándares de la industria estrictos para la seguridad y privacidad.

Las certificaciones incluyen:

- FIPS 140-2 CAVP
- Perfil de Protección de Fundamentos de Dispositivos Móviles del NIAP/Criterios Comunes
- Guía de Implementación de Seguridad Técnica (STIG) de DISA
- Regulación de Protección de Datos Generales (GDPR)

Para obtener más información, por favor, visite
motorolasolutions.com/ion

MOTOROLA SOLUTIONS

MOTOTRBO ION