CHECK POINT
SEGURIDAD MÓVIL

potencia tu información

La detección precisa de amenazas y la respuesta eficiente son componentes críticos para prevenir ataques avanzados en teléfonos inteligentes y tabletas. Las soluciones tradicionales de reputación de aplicaciones y antivirus pueden identificar amenazas conocidas, pero no pueden detectar malware o vulnerabilidades de día cero en redes, sistemas operativos y aplicaciones.

Solo las soluciones que pueden analizar el comportamiento de los tres vectores en busca de indicadores de ataque pueden proteger los dispositivos móviles de manera efectiva para mantenerlos a salvo de los cibercriminales. Check Point SandBlast Mobile identifica amenazas utilizando algoritmos en el dispositivo, en la red y en la nube, activando respuestas de defensa automáticas que mantienen protegidos los dispositivos móviles y los datos en ellos.

LA SEGURIDAD CONSOLIDADA EN DISPOSITIVOS

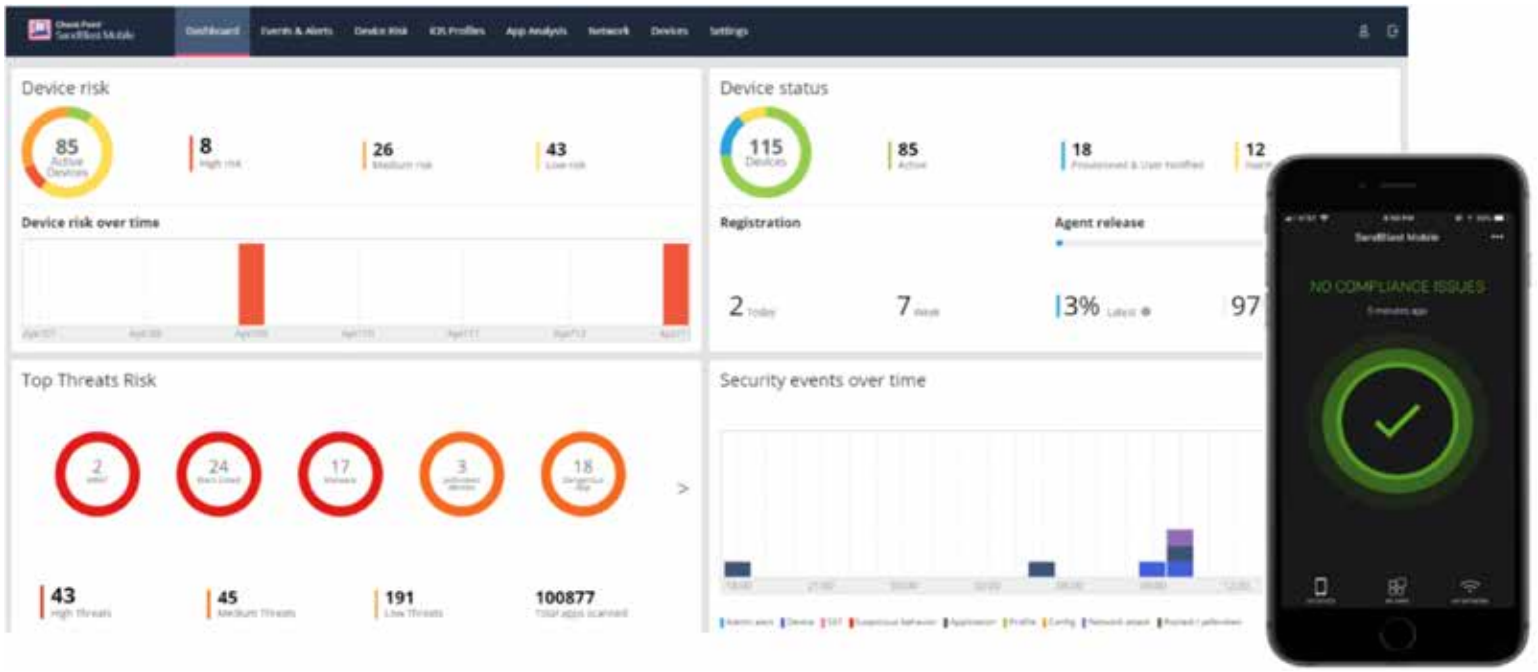
- Interoperability
- Data Security
- Access Control & Secure Communication
- Advanced Threat Prevention
- Endpoint Detection & Response (EDR)
- Mobile Threat Defense

Proporciona un sistema integral para prevenir, detectar y remediar proactivamente los ataques evasivos de malware.

¿CÓMO PUEDE AYUDARME CHECK POINT?

Check Point SandBlast MOBILE

potencia tu información



¿Qué puede monitorear?

- Firmas y orígenes de las aplicaciones para determinar si una aplicación viene de una tienda válida
- Aplicaciones nuevas y actualizaciones instaladas en los dispositivos
- Adquisición de la aplicación desde la tienda o desde el dispositivo cuando no hay un hash exacto en la tienda
- Estado de la conexión de Wi-Fi
- Integridad del sistema operativo, incluyendo validación de root o jailbreak
- Configuración del dispositivo
- Indicadores de compromiso relacionados con exploits
- Información de integridad de conexiones con TLS en una conexión Wi-Fi
- URLs y dominios maliciosos que fueran bloqueados por Anti-phishing, navegación segura y anti-bot
- Eventos de bloqueos de accesos condicionales

Detección y prevención por SandBlast Mobile:

Network Analysis
SandBlast Mobile detecta ataques MiTM, los cuales podrían provocar una fuga de datos sensibles y dejarlos disponibles a los ojos del cibercrimen.

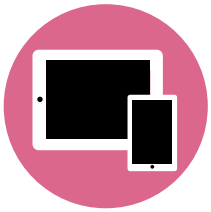
On-device Network Protection
SandBlast Mobile inspecciona y controla todo el tráfico de red en el dispositivo para validar que las URL enviadas al dispositivo no sean maliciosas y cumplan con la política de la compañía. SandBlast Mobile logra esta protección mediante la instalación de un perfil VPN que recorre el tráfico de red de fondo para ser inspeccionado por la policía de SandBlast Mobile.

Configuration Analysis
Los cambios en las configuraciones del dispositivo pueden ocurrir por varias razones. Los usuarios pueden hacer o aceptar cambios al instalar aplicaciones, las organizaciones comerciales pueden requerir cambios para cumplir con los requisitos de la política, o los ciberdelincuentes pueden hacer cambios para llevar a cabo un ataque.

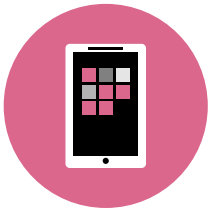
Advanced Root Anlysis
En lugar de solo buscar indicadores estáticos como archivos de superusuario, SandBlast Mobile Protect utiliza técnicas avanzadas para detectar si se concede acceso root en un dispositivo y cómo lo hace, incluido un comportamiento inesperado del sistema operativo que puede indicar rooting o jailbreak.

Behavioral Risk Engine
Check Point SandBlast Mobile utiliza un motor de riesgo conductual (BRE) basado en la nube para realizar un análisis de amenazas en profundidad. Además de los datos de red, configuración y análisis root que recopila, SandBlast Mobile Protect envía información sobre aplicaciones en un dispositivo al BRE. Utiliza estos datos para analizar y detectar actividades sospechosas y produce una puntuación de riesgo basada en el tipo y la gravedad del riesgo. El puntaje de riesgo se usa para determinar qué acción de mitigación automática se necesita para mantener un dispositivo y sus datos protegidos.

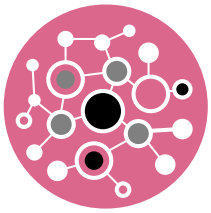
Remediación



On-Device Network Protection
La tecnología anti-bot proporciona los amenazas de C2 y exfiltración de datos. La característica de Conditional Access protege los activos corporativos y los datos de ser accedidos por dispositivos en riesgo. El endurecimiento de políticas y de Conditional Access proporciona un alcance de seguridad en capas independiente y en coperación con soluciones UEM.



UEM Actions
Las soluciones UEM administran dispositivos con políticas estáticas que no cambian con la postura de seguridad de un dispositivo. A través de la integración con estos sistemas, Sandblast Mobile modifica automáticamente accesos privilegiados para reflejar los niveles de riesgo actuales, transformando una gestión de políticas estática en una protección de dispositivos activa.



Network-Based Mitigation
La protección de dispositivos activa proporciona bloqueos on-demand de malware para proteger de ataques nuevos, emergentes y dirigidos, spyware, ataques tipo drive-by y ataques MiTM.

DESCARGA:
LA GUÍA DE SEGURIDAD MÓVIL EMPRESARIAL DE CHECK POINT

DA CLICK AQUÍ PARA CONOCER MÁS
SOLUCIONES SANDBLAST MOBILE

CENTRO
Filadelfia 128, Oficina 602
Col. Nápoles
Alcaldía Benito Juárez
México CDMX 03810

CONMUTADOR
+52.55.5202 5010
comercial@circulodaat.mx
circulodaat.mx

NORTE
+52.81.4159 0580
Penthouse 1, Edificio III Moll del Valle
Calzada del Valle 400
Col. Del Valle
San Pedro Garza, García