Lookout

Seguridad móvil

Introducción

Enero 2025

La necesidad de seguridad móvil

Puntos clave

1. A diferencia de las PC y las computadoras portátiles, la mayoría de los dispositivos móviles permanecen desprotegidos contra el continuo aumento de los ataques cibernéticos.
2. Hoy en día, más de la mitad de los dispositivos que usan los empleados para acceder a los datos de la empresa ejecutan los sistemas operativos móviles iOS, Android o Chrome.
3. Como resultado, los dispositivos móviles se han convertido en un punto de entrada clave para los ciberataques.
4. Muchas organizaciones siguen expuestas con una protección mínima o inadecuada* contra las amenazas móviles
5. Proteger los dispositivos móviles se ha convertido en un requisito obligatorio en muchos marcos de seguridad cibernética

*un MDM no es una solución de seguridad móvil

Lookout

Panorama de amenazas móviles

Ejemplos de detecciones de amenazas y respuesta

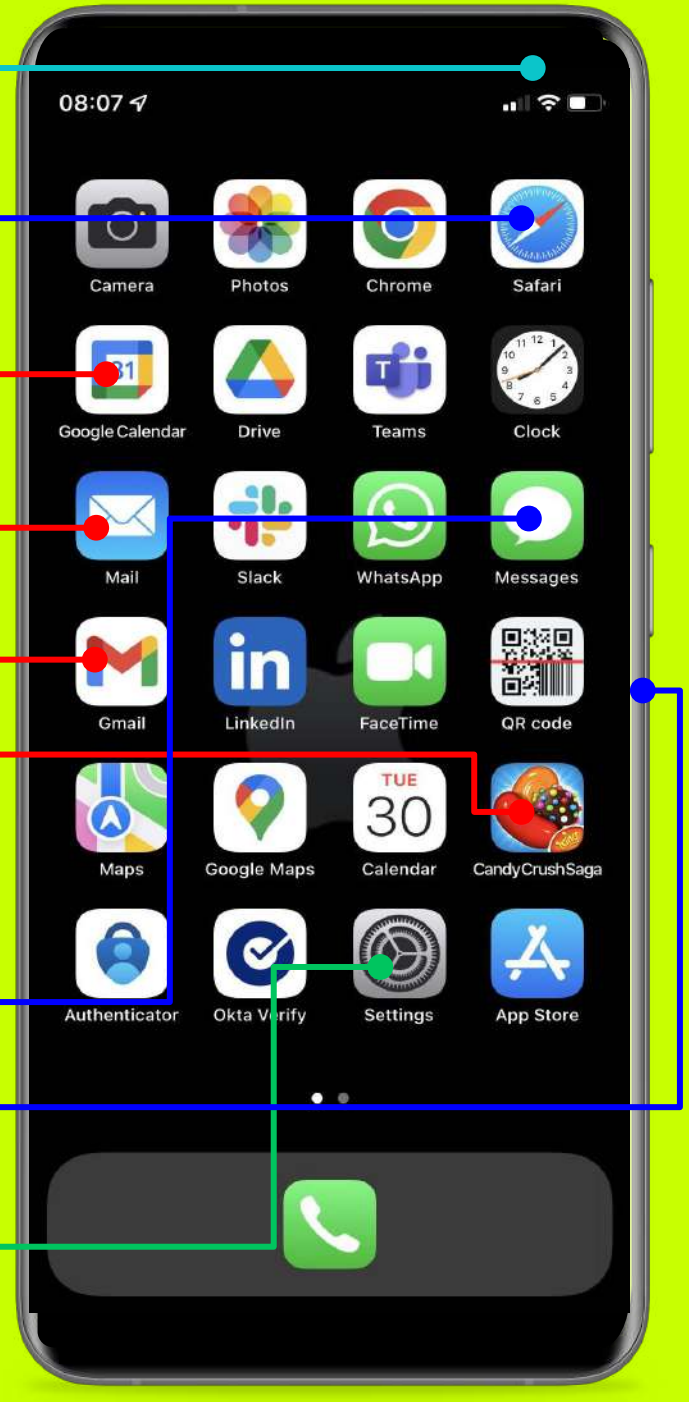
Comprendiendo el riesgo móvil

Puntos de entrada potenciales

Los dispositivos móviles a menudo recopilan datos personales y corporativos y, por lo general, se dejan desprotegidos.

Estas minicomputadoras se han convertido en el objetivo obvio y el camino de menor resistencia para ejecutar ciberataques exitosos.

Redes	Redes WiFi no seguras o puntos de acceso
Aplicaciones	Mezcla de datos personales y corporativos
	Aplicaciones que filtran o transfieren datos
	Aplicaciones descargadas o dañinas
Contenido web	Contenido web dañino
	Ataques de phishing
	Escaneo de códigos QR
Dispositivo	Sistemas operativos obsoletos



Lookout

Impacto potencial de un ciberataque

Siguiendo la cadena de exterminio móvil

Paso 1:
Dispositivo comprometido

El punto de entrada inicial en dispositivos móviles podría provenir de un ataque de phishing, malware incrustado en una aplicación, conexión a una red insegura o mediante una vulnerabilidad de dispositivo explotable. Las amenazas son cada vez más avanzadas y el spyware móvil se puede enviar al dispositivo de forma silenciosa.

Paso 2:
Robo de credenciales

Por lo general, a través de un ataque de phishing exitoso, las credenciales de usuario comprometidas otorgan al atacante las claves de los datos confidenciales o corporativos.

Paso 3:
Ejecutar ransomware

Una vez que se obtiene el acceso, se puede ejecutar malware dañino como el ransomware para desconectar una red de TI completa, negando a una organización el acceso a su propio recurso corporativo hasta que se pague la demanda de rescate de los atacantes.

Etapa 4:
Filtración de datos

Los datos confidenciales son el objetivo lucrativo para un atacante. Las filtraciones de datos generan un impacto en la reputación de una empresa y multas de cumplimiento significativas si surgen discrepancias regulatorias.

Lookout

Acerca de Lookout

Seguridad desde dispositivos a la nube para la forma moderna de trabajar

Lookout se enfoca en proteger los datos comerciales dondequiera que fluyan, brindando protección de datos que permite que las personas y las empresas prosperen.

Lookout está en una posición única para proteger toda la ruta de datos desde el punto final hasta la nube desde una única plataforma de seguridad unificada basada en la nube.

Las empresas, los gobiernos y millones de personas de todo el mundo confían en Lookout para proteger sus datos.

Alcance global

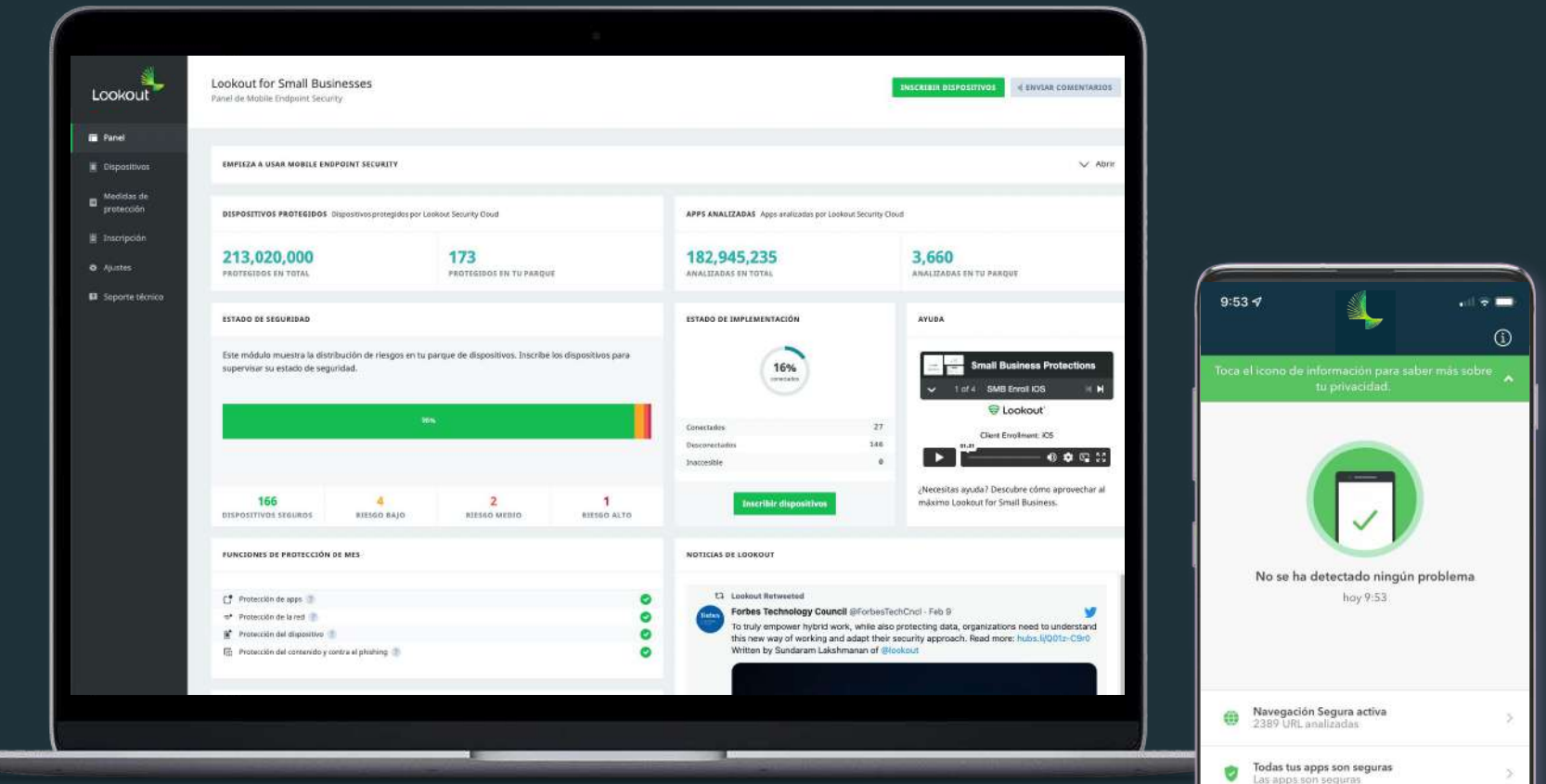
Miles de 6k Negocios en todo el mundo	220m+ Datos personales de las personas físicas	205m+ dispositivos móviles
345M+ aplicaciones móviles	16.5k aplicaciones SaaS	500+ familias de amenazas

Experiencia del cliente

Descripción general del producto, flujo de activación y privacidad

Seguridad móvil de Lookout

Descripción del producto



Consola de administrador de Lookout

- Detecciones de amenazas e información
- Despliegue de control (gestionado/no gestionado)
- Definición de políticas de seguridad
- Configuración integraciones
- Vista de administración móvil para pymes

Aplicación móvil Lookout for Work

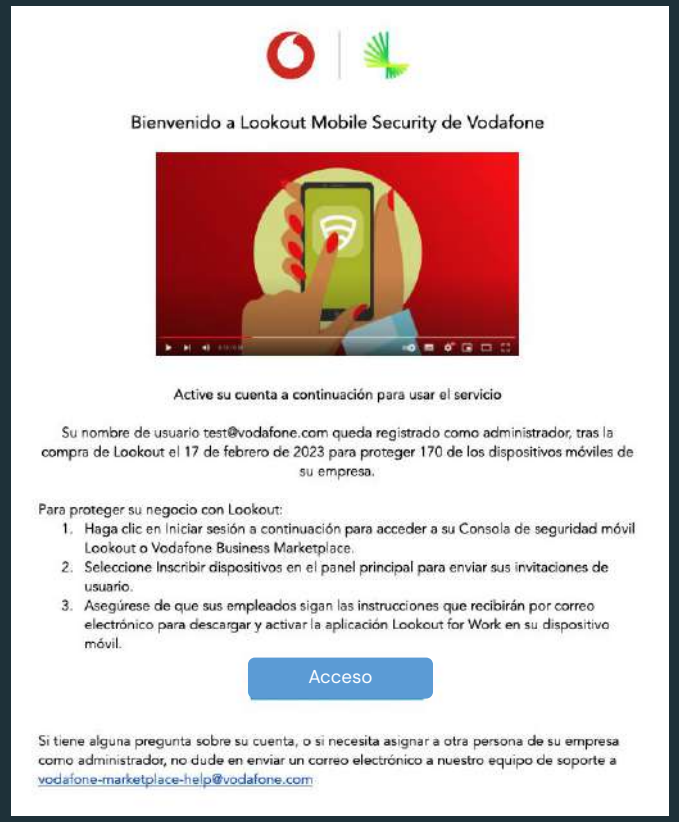
- Compatible con iOS, Android y Chrome OS
- Alertas de amenazas en tiempo real
- Aplicación ligera - bajo consumo de batería
- Pasos de remediación simples
- Garantía de privacidad y educación del usuario

Lookout

Experiencia de activación (1)

Pasos sencillos para proteger a sus usuarios móviles

El cliente recibe un correo electrónico de bienvenida automatizado. Hay instrucciones claras y un "enlace rápido" para iniciar sesión en el servicio de Lookout



Bienvenido a Lookout Mobile Security de Vodafone

Active su cuenta a continuación para usar el servicio

Su nombre de usuario test@vodafone.com queda registrado como administrador, tras la compra de Lookout el 17 de febrero de 2023 para proteger 170 de los dispositivos móviles de su empresa.

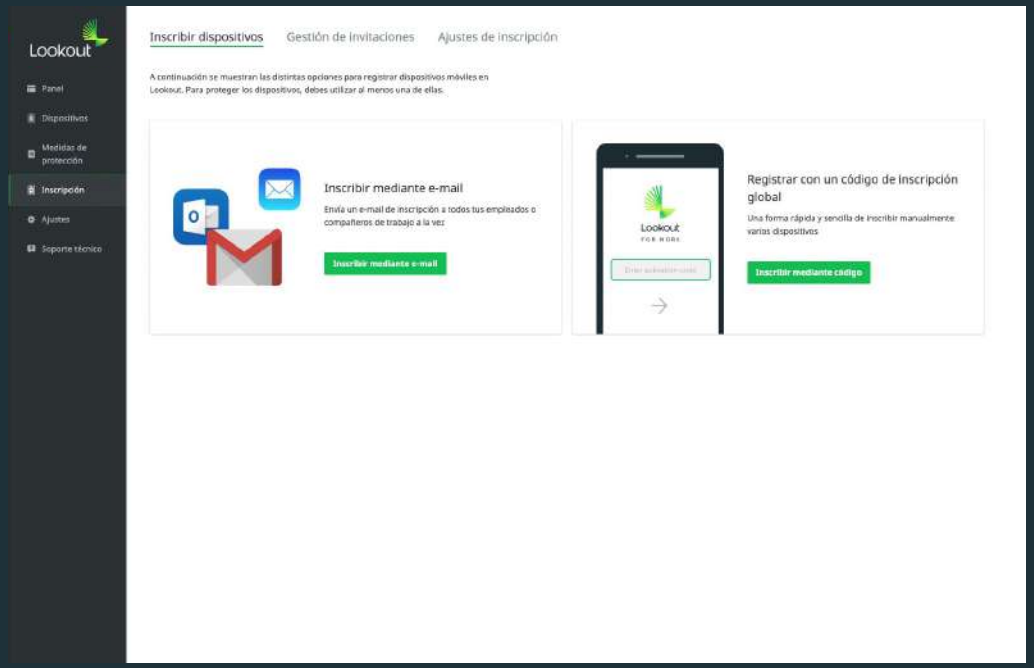
Para proteger su negocio con Lookout:

1. Haga clic en Iniciar sesión a continuación para acceder a su Consola de seguridad móvil Lookout o Vodafone Business Marketplace.
2. Seleccione Inscribir dispositivos en el panel principal para enviar sus invitaciones de usuario.
3. Asegúrese de que sus empleados sigan las instrucciones que recibirán por correo electrónico para descargar y activar la aplicación Lookout for Work en su dispositivo móvil.

Acceso

Si tiene alguna pregunta sobre su cuenta, o si necesita asignar a otra persona de su empresa como administrador, no dude en enviar un correo electrónico a nuestro equipo de soporte a vodafone-marketplace-help@vodafone.com

Navegue a la pestaña Inscripción y elija el método preferido para comenzar a agregar usuarios

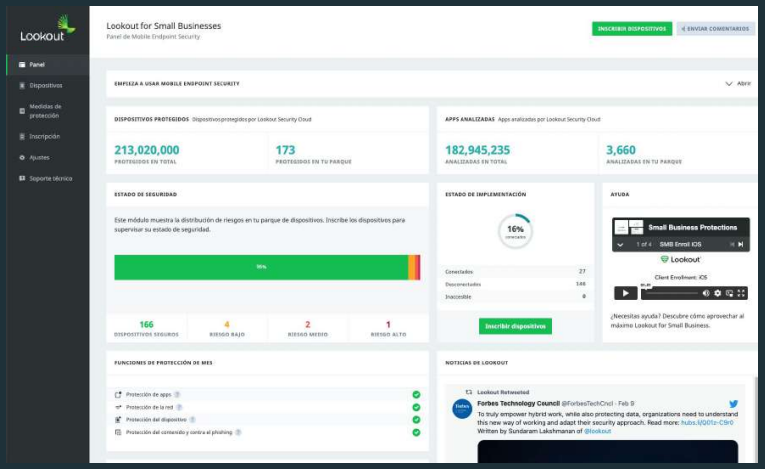


Experiencia de activación (2)

Pasos sencillos para proteger a sus usuarios móviles

Según el método de inscripción preferido, los usuarios reciben instrucciones claras sobre los pasos sencillos que deben seguir

Se informa a los usuarios que la inscripción está completa y están protegidos



Los dispositivos inscritos se muestran en la consola web, lo que brinda visibilidad comercial y opciones de administración de seguridad.

Lookout en acción

Proporcionar protección continua en dispositivos móviles

Lookout brinda protección contra **aplicaciones maliciosas, conexiones de red peligrosas, amenazas basadas en dispositivos e intentos de phishing**

Se proporcionan notificaciones claras que informan al usuario sobre la acción que realiza Lookout cuando se detectan amenazas

Lookout

Respeto a la privacidad del usuario

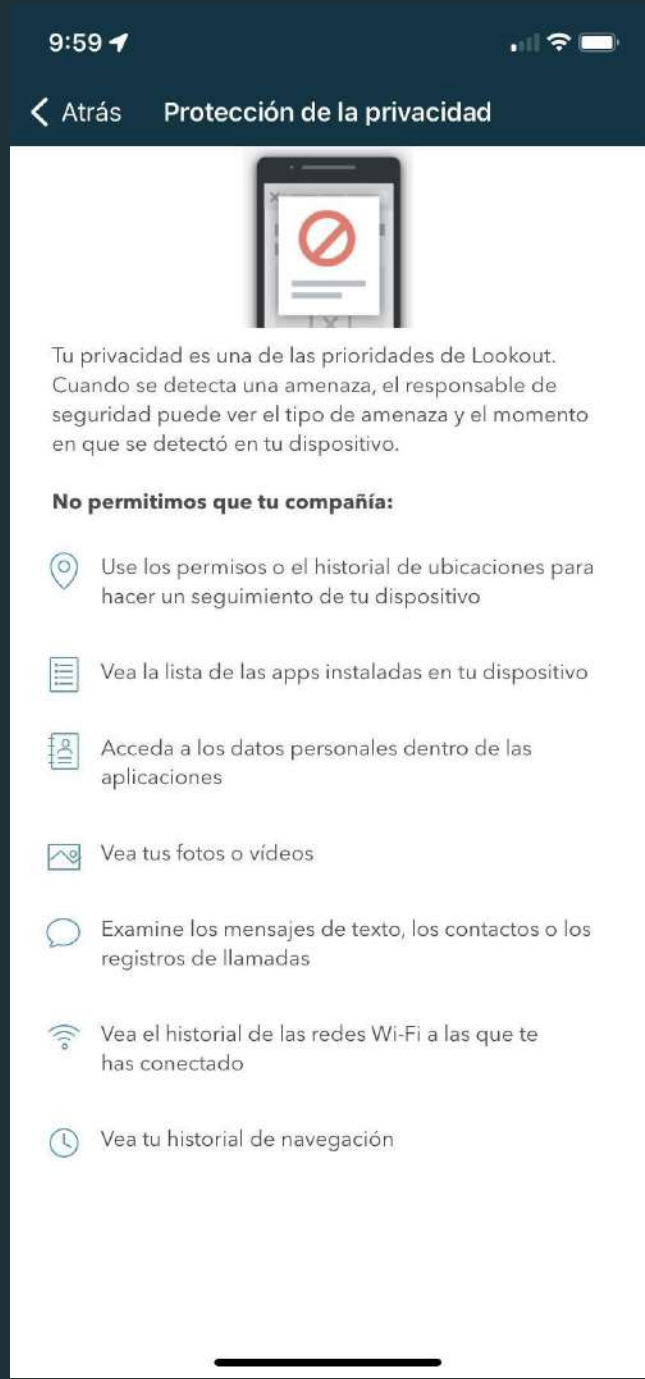
Qué datos recopila Lookout y por qué

La plataforma de seguridad de Lookout se basa en el respeto y la protección de la privacidad personal, recopilando solo los datos necesarios para brindar una seguridad sólida.

Lookout no retiene ni pasa datos personales al administrador.

Lookout recopila seis clases de datos de los dispositivos móviles inscritos:

Datos recolectados	¿Por qué?
Metadatos de la aplicación	Para identificar amenazas de seguridad basadas en aplicaciones
Datos de firmware/OS	Para detectar firmware comprometido u O/S vulnerable
Datos de configuración	Para detectar perfiles de configuración riesgosos o maliciosos
Identificador de dispositivo	Habilite la comunicación del usuario final para detectar y remediar
Datos de contenido web	Para bloquear el acceso a contenido web malicioso o phishing
Datos de seguridad de la red	Habilite decisiones para protegerse contra ataques a la red



Lookout

Detección de phishing

Experiencia de usuario

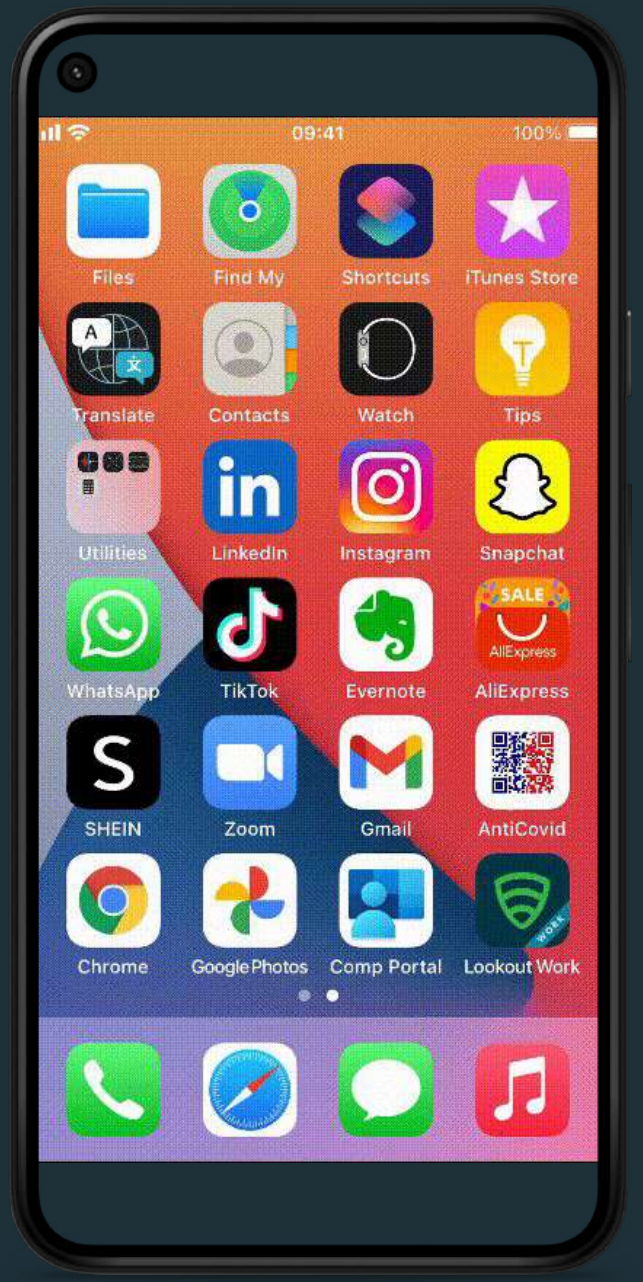
El 85% de los ataques de phishing en dispositivos móviles ocurren fuera del correo electrónico

Lookout detectará y bloqueará la navegación del usuario a un sitio de phishing, lo que automáticamente mantendrá seguros el dispositivo, el usuario y la organización.

Los administradores no recibirán una alerta por correo electrónico

En más del 25 % de los dispositivos de los clientes de Vodafone con Lookout instalado, se detectaron y bloquearon amenazas web y basadas en contenido dañino durante el último trimestre

Medido en la base de clientes de VFIT, VFUK, VFDE, VFNL Lookout (octubre-diciembre de 2022)



Lookout

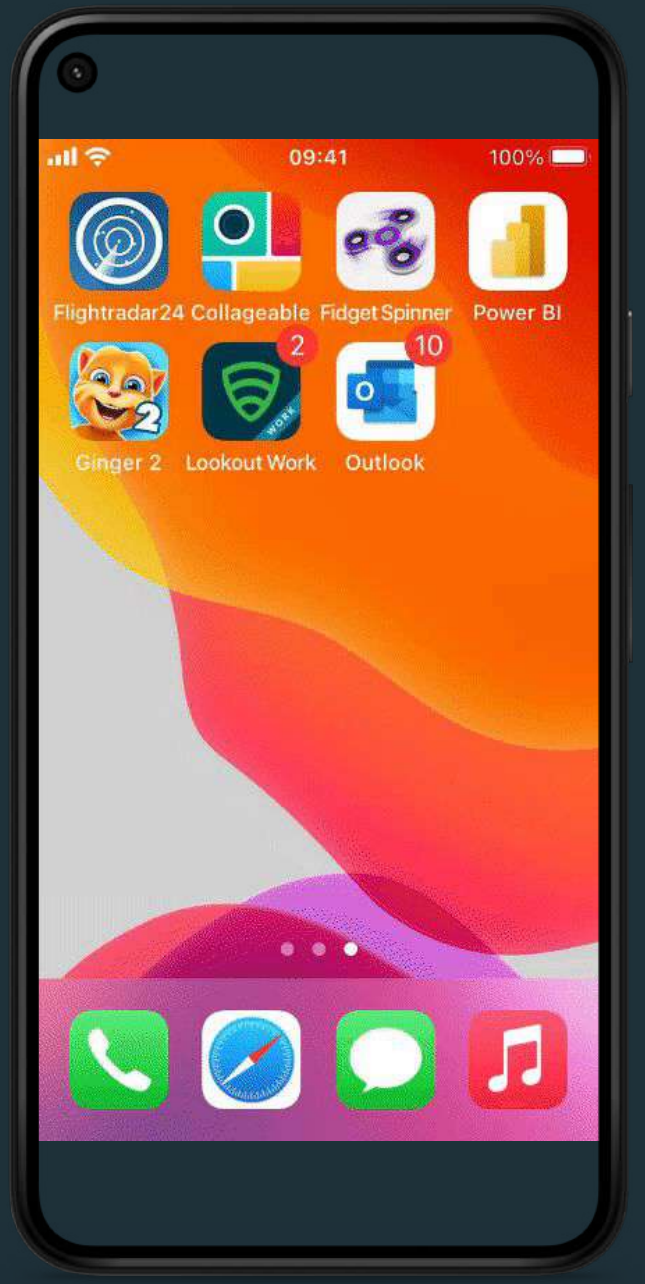
Detección de malware

Experiencia de usuario

Lookout vio un aumento del 120% en las amenazas de aplicaciones móviles de 2021 a 2022

Tras la detección, Lookout notifica al usuario de la misma y proporciona instrucciones sobre la solución recomendada.

Junto con una integración de MDM, los administradores pueden bloquear automáticamente el acceso del usuario a los recursos corporativos hasta que solucionen el problema.



Lookout

Tasas de encuentro de amenazas móviles

Evidencia de que los ataques móviles van en aumento

Q4 2022	Android	iOS
Phishing	12.1%	25.2%
OS Vulns	0.57%	7.55%
App Threats	0.85%	0.86%
Device Risks	8.62%	3.98%
App Risk	0.20%	0.43%
Network Threats	0.16%	0.15%
App Vulns	18.95%	1.37%

Base instalada global de Lookout

Dispositivos móviles que han encontrado una o más amenazas por trimestre

Datos de Lookout: capturados en febrero de 2023

Lookout

Comparación de Lookout vs MDM

Hay brechas de seguridad con MDM

Sin protección con MDM

Protección parcial/limitada

Protección proporcionada por MDM

La matriz de riesgos de Lookout Mobile muestra las áreas de exposición cuando solo se implementa una solución MDM/UEM.

La función principal de un MDM es administrar dispositivos móviles, como empujar o exigir aplicaciones y funciones de seguridad básicas como bloqueo o borrado remoto.

Lookout agrega una capa de seguridad necesaria para detectar y proteger contra amenazas entrantes como phishing o malware.

	WEB & CONTENT	APPS	NETWORK	DEVICE
AMENAZAS	Suplantación de identidad Descargas automáticas Páginas web maliciosas y archivos	Spyware y software de vigilancia Troyanos Otras aplicaciones maliciosas	Ataque de intermediario Torres de telefonía falsas Instalación de Certificados raíz	Escalación de privilegios Jailbreak/Root remoto
SOFTWARE VULNERABILIDADES	Contenido malformado que desencadena vulnerabilidades del sistema operativo o de la aplicación	Aplicaciones desactualizadas SDK vulnerables Malas prácticas de codificación	Vulnerabilidades de hardware de red Vulnerabilidades de la pila de protocolos	SO desactualizado Hardware sin salida Vulnerable aplicaciones preinstaladas
CONDUCTA & CONFIGURACIONES	Abrir archivos adjuntos y visitar enlaces a contenido potencialmente no seguro	Aplicaciones que filtran datos Aplicaciones que infringen la seguridad de la empresa Aplicaciones que infringen el cumplimiento	Proxies, VPN, Certificados Raiz Conexión automática a redes sin cifrar	Jailbreak/root iniciado por el usuario Sin código PIN/contraseña depuración USB

Lookout

Lookout y MDM

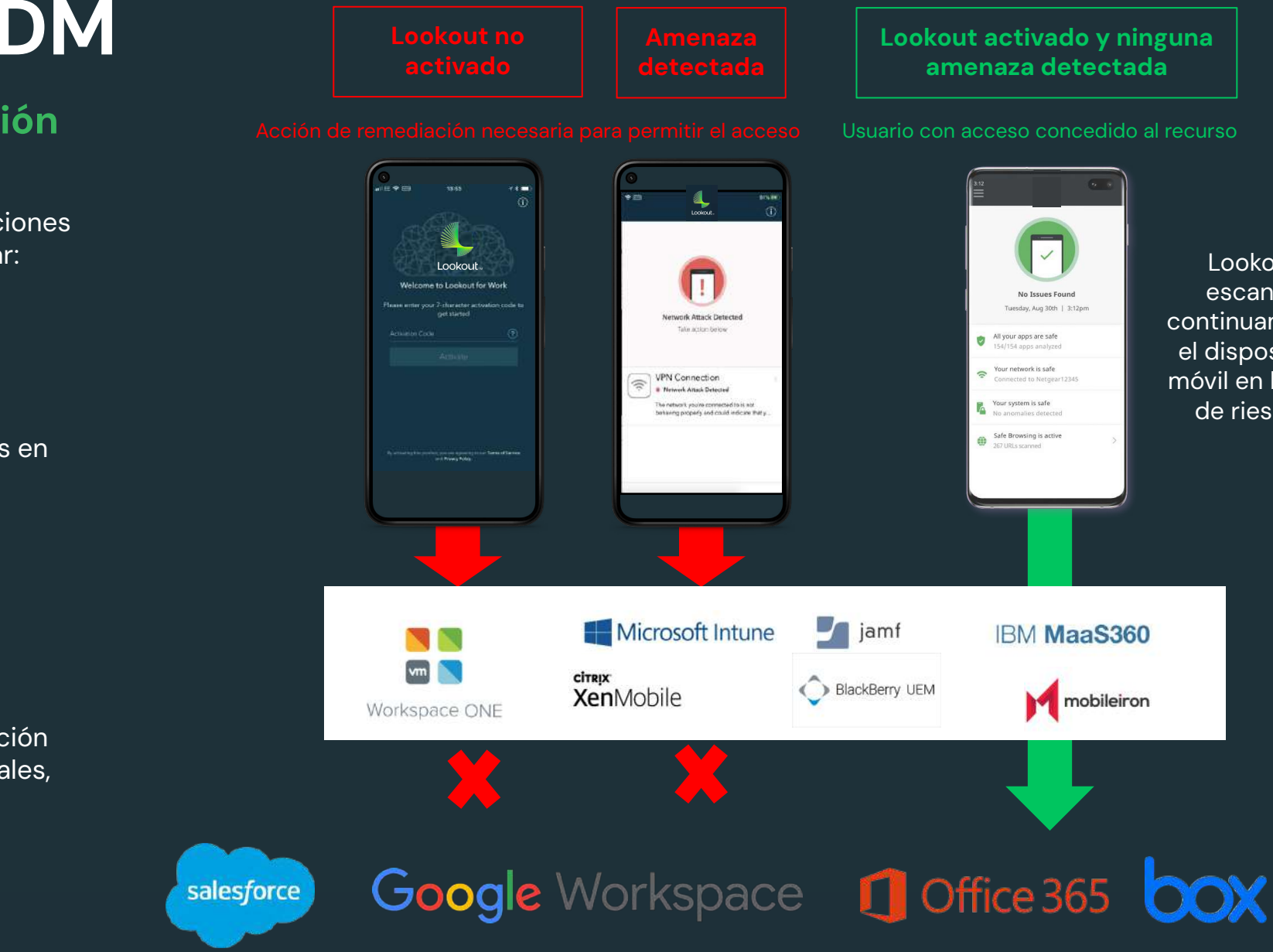
Beneficios de la integración

Lookout se integra con todas las soluciones líderes de MDM/UEM para desbloquear:

Control de acceso basado en riesgos
La tranquilidad de saber que solo los dispositivos móviles seguros pueden acceder a los recursos corporativos, introducir políticas de acceso basadas en el nivel de riesgo

Activación forzada
Solicite la activación de la aplicación Lookout antes de que se conceda el acceso a los recursos corporativos

Activación con cero clic
Implemente silenciosamente la aplicación Lookout for Work para los usuarios finales, aceptando permisos en su nombre



Lookout

Comparación de productos y precios

Productos y precios

Lookout Mobile Endpoint Security

Lookout Mobile Endpoint Security (MES) Características	PCP Only	Small Business	MES Essentials	MES Advanced
Protección contra amenazas web y contenido dañino (incluye phishing)				
Protección contra amenazas en apps				
Protección contra amenazas en la red				
Protección contra amenazas en el dispositivo				
Integraciones (MDM / UEM / IAM / SIEM)				
Accesos Confianza Cero / Acceso condicional continuo				
Administración de vulnerabilidades y parches de seguridad				
Analisis a profundidad de apps y lista de apps no permitidas				

¿Por qué Lookout?

El líder del mercado reconocido

230M
MOBILE DEVICES

345M
APPS ANALYZED

4.5B+
WEB ITEMS ANALYZED

MACHINE INTELLIGENCE

500M+
PHISHING SITES/DAY

10K+
MALICIOUS APPS/DAY

Conjunto de datos globales

Lookout ha acumulado un conjunto de datos de amenazas globales de más de 210 millones de dispositivos móviles y 185 millones de aplicaciones, que tenemos en Lookout Security Cloud. A través del aprendizaje automático y la inteligencia predictiva, proporcionamos los niveles más altos posibles de eficacia de seguridad.

Pioneros e innovadores

Lookout definió la categoría Seguridad Móvil con productos innovadores para abordar el panorama de amenazas móviles. Aplicamos este conocimiento y experiencia a los datos, la privacidad y la identidad de las personas, desde pymes hasta grandes empresas.

Enfoque de pequeñas empresas

Nuestro conjunto de productos MES incluye Lookout para pequeñas empresas, que está optimizado para organizaciones de menor tamaño. Esta solución personalizada se vende activamente a escala a pequeñas empresas que carecen de experiencia en seguridad, en múltiples mercados.

Nuestros clientes

Con la confianza de organizaciones líderes

CONTACTO

GLOBAL INTERACTIVE GROUP SRL.
&
ENFORCE ONE S.A.

Dirección

Alicia Moreau de Justo N* 740, Piso 3 of. 1
Puerto Madero, Buenos Aires. Argentina.

Contacto

+549 11 6 743 6697

info@gigsrl.com

www.gigsrl.com

Global INTERACTIVE GROUP

ENFORCE ONE S.A.