MobileIron

Data sheet de MobileIron Threat Defense

Información general

MobileIron Threat Defense ofrece una seguridad móvil sin precedentes que permite a las organizaciones detectar y remediar los ciberataques en dispositivos, redes y aplicaciones. Con un solo agente inteligente, las organizaciones pueden proteger los activos de la empresa contra las amenazas móviles conocidas y de día cero con algoritmos de aprendizaje automático.

La implementación y la activación de Threat Defense en dispositivos móviles se realiza de forma silenciosa en dispositivos administrados y no administrados sin necesidad de que los usuarios hagan nada, lo que se traduce en una adopción del 100 % por parte de los usuarios. La corrección de amenazas se realiza en el dispositivo, incluso sin conexión a Internet.

No se interrumpe la productividad de los usuarios en los dispositivos y se evita que los dispositivos móviles afectados tengan un impacto en la red corporativa y se corra el riesgo de perder datos. Una vez activada en el dispositivo, el usuario no puede eliminar ni desactivar la protección contra las amenazas.

Principales ventajas

MobileIron Threat Defense es una solución diseñada para dispositivos móviles y emplea algoritmos de aprendizaje automático optimizados para ejecutarse de forma continua en el dispositivo, lo que le permite detectar amenazas incluso cuando el dispositivo no está conectado.

Sencilla

Al ser una sola aplicación, le facilita las cosas gracias a la protección integrada en su cliente de MobileIron. Además, también es una solución sencilla para sus usuarios, que no tendrán que hacer nada para activar el cliente.

Informativa

Cuente con visibilidad inmediata y constante de las amenazas malintencionadas que haya en todos los dispositivos móviles, así como con los análisis detallados de las aplicaciones peligrosas.

En el dispositivo

Obtenga una detección y una corrección sin precedentes contra amenazas ya conocidas y de día cero con algoritmos de aprendizaje automático en el dispositivo sin necesidad de conexión a Internet.

Acerca de MobileIron

MobileIron proporciona una base segura para el trabajo moderno. Para obtener más información, visite www.mobileiron.com.

MKT ES-ES v2.1

CARACTERÍSTICA	DESCRIPCIÓN	VENTAJA	Sistema operativo	
			iOS	
Integración de UEM	Solución integrada de protección contra amenazas incluida en la administración unificada de puntos de conexión.	El departamento informático solo necesita administrar y mantener una aplicación, lo que reduce los costes operativos.	Sí	Sí
Implementación automática	El administrador puede implementar automáticamente el cliente y activar Threat Defense en los dispositivos seleccionados.	100 % de adopción por parte de los usuarios.	Sí	Sí
Detección de amenazas	**Vulnerabilidades del dispositivo** • Jailbreak • Detección de descifrados • Versión de SO vulnerable • Versión de SO mínima • Cifrado desactivado • Contraseña eliminada/desactivada • Manipulación del sistema de archivos • Perfiles no confiables/sospechosos • Elevación de privilegios **Vulnerabilidades de la red** • Ataques de intermediarios (*Man in the Middle*) • Puntos de acceso maliciosos • Wi-Fi no segurizada • Bluetooth malicioso • Puntos de acceso no autorizados • Portal cautivo **Vulnerabilidades de la aplicación** • Evaluación de alto riesgo para la privacidad • Evaluación de riesgos para la alta privacidad • Comportamiento sospechoso de una aplicación • Aplicaciones de carga lateral	Detecte amenazas conocidas y amenazas de día cero en el dispositivo mediante algoritmos de aprendizaje automático. Mayor visibilidad y conocimiento de las vulnerabilidades y amenazas de los dispositivos, los sistemas operativos, las redes y las aplicaciones.	Sí	Sí

Análisis de aplicaciones	• **Visibilidad de la aplicación:** inventario configurable de las aplicaciones instaladas en un dispositivo.
	  • Todas las aplicaciones (iOS)
	  • Aplicaciones administradas
	
	• **Análisis de aplicaciones:** análisis opcional de las aplicaciones sin conexión. Correlacione automáticamente el riesgo de las aplicaciones con el análisis de dispositivos para obtener información sobre:
	  • Contenido: malware
	  • Intención: comportamiento de la aplicación
	  • Contexto: dominios, certificados, código compartido, comunicaciones de red
	
	• **Información de las aplicaciones:** establezca políticas de seguridad para reducir los riesgos
	
	• **Informes:** imprima informes con los resúmenes de los riesgos de seguridad y privacidad de las aplicaciones
	
	• **Carga de aplicaciones:** para el análisis y la calificación del riesgo
		Información sobre qué aplicaciones están instaladas en el dispositivo.
		
		Análisis opcionales con informes detallados de la puntuación de la evaluación de amenazas, explicaciones de los riesgos e implicaciones.
			Sí	Sí

Notificación de amenazas	El administrador selecciona las amenazas para las que desea que se envíe una notificación al usuario del dispositivo una vez que se detecte una amenaza en el servidor. Los mensajes se pueden personalizar y crear en varios idiomas.	Notificación al dispositivo configurable sobre las amenazas detectadas en el dispositivo.	Sí	Sí
Notificación de amenazas locales	Cree múltiples configuraciones de acción local utilizando la lista de amenazas actual que se importa automáticamente. El sistema notifica al administrador cuando hay una nueva lista de amenazas disponible e identifica las amenazas que se han eliminado de la lista.	El administrador controla la cantidad y el contenido de la información sobre las amenazas detectadas que se muestra a los usuarios de los dispositivos. El idioma de las notificaciones de las amenazas coincide con el idioma seleccionado para el dispositivo.	Sí	Sí

Medidas de corrección	• Cree múltiples configuraciones de medidas de corrección locales utilizando la lista de amenazas actual que se importa automáticamente.
	
	• El administrador selecciona la acción que se debe realizar por plataforma para cada amenaza enumerada en la lista importada.
	
	• **Medidas de cumplimiento iniciadas por el servidor**
	  • Supervisión
	  • Envío de alertas
	  • Bloqueo de AppConnect y del correo electrónico
	  • Cuarentena
	  • Borrado selectivo
	  • Cumplimiento por niveles (respuesta automatizada y gradual)
	
	• **Medidas locales en Android:**
	  • Cuarentena: eliminar toda la configuración
	  • Cuarentena: eliminar toda la configuración excepto la conexión Wi-Fi cuando solo haya Wi-Fi
	  • Eliminar toda la configuración excepto la conexión Wi-Fi
	  • Eliminar las aplicaciones administradas y bloquear la descarga
	  • Desactivar el Bluetooth
	  • Desconectar la Wi-Fi
	  • Retirar y borrar
	
	• **Medidas locales en iOS:**
	  • Bloqueo de las aplicaciones de AppConnect
	  • Tráfico de red *sinkhole*
	
	• **El sistema envía una notificación al administrador cuando hay una nueva lista de amenazas disponible**
		Las acciones de cumplimiento y las notificaciones de amenazas se realizan en dispositivos con o sin conexión a Internet.
		
		Transforma el dispositivo móvil en el punto de cumplimiento de políticas para reducir el tiempo de detección de amenazas y de ataques, y acortar significativamente la «cadena de ataque» de los ataques que tienen su origen en dispositivos móviles.
		
		La política de cumplimiento local siempre está actualizada con la lista actual de amenazas detectadas en el dispositivo, lo que ahorra tiempo y reduce los errores humanos.
		
		Se pueden crear múltiples configuraciones de corrección local y aplicarlas a diferentes grupos de usuarios.
			Sí	Sí

Escaneo de dispositivos para detectar amenazas	Ejecute escaneos contínuos en busca de amenazas.	Reduzca el tiempo entre la detección y la corrección de las amenazas móviles.	Sí	Sí
	Ejecute el escaneo cuando el dispositivo se registre.	Optimiza la protección y la duración de la batería.	Sí	Sí
Consola de administración	Integración de la zConsole basada en la nube con un servidor de administración unificada de puntos de conexión.	Administre fácilmente los dispositivos corporativos y de propiedad de los empleados.	Sí	Sí

Opciones de implementación	Local, SaaS.	Puede elegir modelo de implementación que se adapte a las necesidades de su empresa.	Sí	Sí
Ubicación del alojamiento	Servidores ubicados en las principales regiones geográficas del mundo.	Puede elegir la ubicación para satisfacer los requisitos de privacidad de datos y minimizar la latencia.	Sí	Sí
Controles de la política de privacidad de datos	Políticas de privacidad de datos configurables para controlar la divulgación de información de identificación personal (IIP).	Facilita el cumplimiento de la empresa con el RGPD, las mejores prácticas del sector y los requisitos OEM de los dispositivos.	Sí	Sí
Escala empresarial probada	>250 000 para un solo cliente.	Experiencia de implementación en empresas pequeñas y grandes.	Sí	Sí
Idioma local	Traducido a 14 idiomas.	Fácil de usar.	Sí	Sí

Privacidad

Las políticas de seguridad y bloqueo de UEM correctamente configuradas, junto con MobileIron Threat Defense, proporcionan una estrategia de seguridad de varios niveles con una respuesta automatizada ante las amenazas para ayudar a proteger los datos en reposo y en tránsito de los usuarios móviles que los identifican personalmente.

Asistencia técnica

Consulte las notas de la versión de MobileIron para obtener información sobre especificaciones adicionales del producto.

Licencia

La suscripción a MobileIron Threat Defense es un complemento de la licencia de administración unificada de puntos de conexión y está disponible por usuario o por dispositivo. Póngase en contacto con su representante de cuenta local o con un distribuidor con valor añadido para obtener los precios específicos que mejor se adapten a su empresa.