MobileIron

Foglio dati su MobileIron Threat Defense

Panoramica

MobileIron Threat Defense garantisce una sicurezza unica nel suo genere per i dispositivi mobili, permettendo alle aziende di rilevare e correggere gli attacchi informatici ad applicazioni, reti e dispositivi. Con un unico agente intelligente, le aziende possono proteggere le risorse aziendali dalle minacce mobili note e zero-day grazie ad algoritmi di machine learning.

La distribuzione e l'attivazione di Threat Defense sui dispositivi mobili gestiti e non gestiti viene adottata da tutti gli utenti perché viene eseguita automaticamente e non richiede il loro intervento. La correzione delle minacce avviene sul dispositivo, anche senza una connessione a Internet attiva.

Il lavoro degli utenti sul dispositivo non viene interrotto e ai dispositivi mobili compromessi viene impedito di avere un impatto sulla rete aziendale e di mettere a rischio i dati. Dopo l'attivazione sul dispositivo, la protezione dalle minacce non può essere rimossa o disattivata dall'utente.

Vantaggi principali

MobileIron Threat Defense, appositamente progettato per i dispositivi mobili, utilizza algoritmi di machine learning ottimizzati per essere eseguiti in modo continuo sul dispositivo e per rilevare le minacce anche quando il dispositivo è offline.

Semplice

Una sola app consente di usufruire facilmente della protezione integrata nel client MobileIron. Massima facilità d'uso per gli utenti che non devono intraprendere alcuna azione per attivare il client.

Informazioni dettagliate

Visibilità immediata e continua delle minacce dannose su tutti i dispositivi mobili e analisi dettagliata delle app rischiose.

Sul dispositivo

Gli algoritmi di machine learning sul dispositivo rilevano e correggono le minacce zero-day e note, anche se la connessione a Internet non è attiva.

Informazioni su MobileIron

MobileIron offre un fondamento sicuro per il lavoro moderno. Per ulteriori informazioni, visitare www.mobileiron.com.

MKT IT-IT v2.1

401 East Middlefield Road, Mountain View, CA 94043 • globalsales@mobileiron.com • www.mobileiron.com • Tel: +1.877.819.3451 • Fax: +1.650.919.8006

FUNZIONALITÀ	DESCRIZIONE	VANTAGGIO	Sistema operativo	
			iOS	
Integrazione UEM	Soluzione di protezione dalle minacce integrata nella gestione unificata degli endpoint (UEM).	Gestione e manutenzione IT tramite un'unica app con conseguente riduzione dei costi operativi.	Sì	Sì
Deployment automatico	Gli amministratori possono distribuire il client automaticamente e attivare Threat Defense sui dispositivi selezionati.	Adozione completa da parte degli utenti.	Sì	Sì
Rilevamento delle minacce	**Vulnerabilità del dispositivo** • Jailbreak • Rilevamento root • Versione SO vulnerabile • Versione SO minima • Cifratura disattivata • Password rimossa/disattivata • Manomissione del file system • Profili non attendibili/sospetti • Elevazione dei privilegi **Vulnerabilità della rete** • Attacchi man-in-the-middle • Hotspot dannosi • Wi-Fi non protetta • Bluetooth dannoso • Punti di accesso non autorizzati • Portale bloccato **Vulnerabilità delle applicazioni** • Valutazione della gravità del rischio per la privacy • Valutazione della gravità del rischio per la sicurezza • Comportamento sospetto delle app • Caricamento delle app in sideload	Rilevamento delle minacce note e zero-day sul dispositivo con algoritmi di machine learning. Maggiore visibilità e consapevolezza delle vulnerabilità e minacce per dispositivi, applicazioni, SO e rete.	Sì	Sì

Analisi delle app	• **Visibilità delle app:** inventario configurabile delle applicazioni installate sui dispositivi
	  • Tutte le applicazioni (iOS)
	  • Applicazioni gestite
	
	• **Analisi app:** analisi facoltativa offline delle applicazioni. Confronto automatico del rischio per le app con l'analisi dei dispositivi finalizzato a fornire informazioni su:
	  • Contenuti: malware
	  • Intenti: comportamento app
	  • Contesti: domini, certificati, codice condiviso, comunicazioni di rete
	
	• **Intelligence delle app:** impostazione di policy di sicurezza per ridurre il rischio
	
	• **Rapporti:** stampa di rapporti di riepilogo sulla sicurezza delle app e sul rischio per la privacy
	
	• **Caricamento delle applicazioni:** per l'analisi e la valutazione dei rischi
		Informazioni su quali app sono installate sui dispositivi.
		
		Analisi facoltativa con rapporti dettagliati su punteggi di valutazione dei rischi, descrizione dei rischi e implicazioni.
			Sì	Sì

Notifica delle minacce	L'amministratore seleziona le minacce per le quali desidera che sia inviata una notifica agli utenti dei dispositivi quando viene rilevata una minaccia sul server. I messaggi possono essere creati e personalizzati in più lingue.	Notifiche configurabili delle minacce rilevate sui dispositivi.	Sì	Sì
Notifica locale delle minacce	Creazione di più configurazioni di azioni locali tramite l'elenco corrente delle minacce importato automaticamente. Il sistema informa l'amministratore quando è disponibile un nuovo elenco delle minacce e identifica le minacce che sono state eliminate dall'elenco.	L'amministratore controlla la quantità e il contenuto delle informazioni sulle minacce rilevate che vengono visualizzati dagli utenti dei dispositivi. La lingua localizzata delle notifiche delle minacce corrisponde alla lingua selezionata per i dispositivi.	Sì	Sì

Azioni di correzione	• Creazione di più configurazioni di azioni di correzione locali tramite l'elenco corrente delle minacce importato automaticamente.
	
	• L'amministratore seleziona l'azione da intraprendere per piattaforma per ciascuna delle minacce indicate nell'elenco importato.
	
	• **Azioni di conformità inziate dal server**
	  • Monitoraggio
	  • Invio di avvisi
	  • Blocco di AppConnect ed e-mail
	  • Quarantena
	  • Cancellazione selettiva
	  • Conformità a livelli (risposta automatica e graduata)
	
	• **Azioni locali su Android:**
	  • Quarantena – Rimuove tutte le configurazioni
	  • Quarantena – Rimuove tutte le configurazioni eccetto quella Wi-Fi quando l'opzione è solo Wi-Fi
	  • Rimozione di tutte le configurazioni eccetto quella Wi-Fi
	  • Rimozione delle app gestite e blocco del download
	  • Disattivazione di Bluetooth
	  • Disconnessione della rete Wi-Fi
	  • Disattivazione e cancellazione
	
	• **Azioni locali su iOS:**
	  • Blocco di app AppConnect
	  • Traffico di rete sinkhole
	
	• **Il sistema informa l'amministratore quando è disponibile un nuovo elenco delle minacce**
		Le azioni di conformità vengono eseguite sui dispositivi e le notifiche vengono inviate indipendentemente dal fatto che la connessione Internet sia attiva o meno.
		
		Trasforma i dispositivi mobili in di applicazione delle policy per ridurre il tempo di rilevamento delle minacce e degli attacchi e per accorciare in modo significativo la "kill chain" degli attacchi originati dai dispositivi mobili stessi.
		
		Poiché la policy di conformità locale è sempre aggiornata con l'elenco corrente delle minacce rilevate sui dispositivi, consente di risparmiare tempo e ridurre gli errori umani.
		
		È possibile creare più configurazioni di azioni di correzione locali e applicarle a diversi gruppi di utenti.
			Sì	Sì

Esegue scansioni dei dispositivi alla ricerca di minacce	Esegue scansioni continue alla ricerca di minacce.	Riduce il tempo che intercorre tra il rilevamento e la correzione delle minacce mobili.	Sì	Sì
	Esegue una scansione quando i dispositivi effettuano il check-in.	Ottimizza la protezione e la durata della batteria.	Sì	Sì
Console di gestione	Integrazione della zConsole basata su cloud con il server di gestione unificata degli endpoint.	Consente di gestire facilmente i dispositivi aziendali e di proprietà dei dipendenti.	Sì	Sì

Opzioni di deployment	Locale, SaaS.	Scelta del modello di implementazione più adatto alle esigenze aziendali.	Sì	Sì
Posizione di hosting	I server sono ubicati nelle principali aree geografiche in tutto il mondo.	Scelta dell'ubicazione per soddisfare i requisiti di privacy dei dati e minimizzare la latenza.	Sì	Sì
Controlli delle policy sulla privacy dei dati	Policy sulla privacy dei dati configurabili per controllare la divulgazione di informazioni di identificazione personale.	Facilita la conformità aziendale con il regolamento GDPR, le best practice del settore e i requisiti OEM dei dispositivi.	Sì	Sì
Scala aziendale comprovata	>250.000 per singolo cliente.	Esperienza di implementazione in aziende di ogni dimensione.	Sì	Sì
Lingua locale	Traduzione in 14 lingue.	Semplice da usare.	Sì	Sì

Privacy
Le policy di blocco e protezione UEM adeguatamente configurate, insieme a MobileIron Threat Defense, offrono una strategia per la sicurezza a più livelli che risponde automaticamente alle minacce e consente di proteggere i data-at-rest e i dati in transito che permetterebbero l'identificazione dell'utente.

Supporto
Consultare le Note di rilascio di Mobileiron per informazioni sulle specifiche aggiuntive del prodotto.

Licenze
La sottoscrizione a MobileIron Threat Defense è un componente aggiuntivo della licenza di gestione unificata degli endpoint (UEM) e può essere acquistata come licenza per utente o per dispositivo. Contattare il rappresentante dell'account locale o il rivenditore a valore aggiunto (VAR) per informazioni che meglio si adattano alle proprie esigenze.