MobileIron

Datenblatt für MobileIron Threat Defense

Übersicht

MobileIron Threat Defense bietet eine unübertroffene Sicherheit für Mobilgeräte und erlaubt es Unternehmen, Hackerangriffe auf Geräte, Netzwerke und Apps zu erkennen und einzugrenzen. Mit einem einzigen intelligenten Agenten können Unternehmen ihre Daten vor bekannten und unbekannten mobilen Bedrohungen mit künstlicher Intelligenz schützen.

Die Bereitstellung und Aktivierung von Threat Defense auf Mobilgeräten erfolgt auf verwalteten und nicht verwalteten Geräten im Hintergrund ohne zusätzliche Eingriffe des Benutzers, das heißt, die Akzeptanz der Benutzer liegt bei 100 %. Die Eingrenzung von Bedrohungen erfolgt direkt auf dem Gerät, selbst wenn keine Internetverbindung vorhanden ist.

Die Benutzerproduktivität auf dem Gerät wird nicht beeinträchtigt; gefährdete Mobilgeräte können nicht auf das Unternehmensnetzwerk zugreifen, sodass keine Datenverluste entstehen. Sobald die Funktion auf dem Gerät aktiviert ist, kann der Benutzer den Schutz nicht mehr entfernen oder deaktivieren.

Hauptvorteile

MobileIron Threat Defense wurde für Mobilgeräte entwickelt und nutzt Algorithmen der künstlichen Intelligenz, die so optimiert sind, dass sie laufend auf dem Gerät aktiv sind und Bedrohungen selbst dann erkennen, wenn das Gerät offline ist.

Einfach

Mit der in dem MobileIron-Client integrierten Schutzfunktion wird die Bedrohungsabwehr ganz einfach. Für Ihre Benutzer ist die Funktion unkompliziert, weil sie keinerlei Maßnahmen zur Aktivierung des Clients ausführen müssen.

Transparent

Sie erhalten sofort und laufend einen transparenten Überblick über Bedrohungen auf allen Mobilgeräten und detaillierte Analysen riskanter Apps.

Auf dem Gerät

Sie erhalten eine bisher nicht möglich gewesene Erkennung und Abwehr bekannter und unbekannter Bedrohungen durch Algorithmen künstlicher Intelligenz auf dem Gerät, ohne dass eine Internetverbindung erforderlich ist.

Über MobileIron

MobileIron bietet die sichere Basis für zeitgemäße Arbeit. Weitere Informationen finden Sie unter www.mobileiron.com.

MKT DE-DE v2.1

FUNKTION	BESCHREIBUNG	VORTEIL	Betriebssystem iOS	Betriebssystem Android
UEM-Integration	Integrierte Lösung zum Schutz vor Bedrohungen in Unified Endpoint Management.	IT-App zur Verwaltung und Pflege zur Senkung der Betriebskosten.	Ja	Ja
Automatische Bereitstellung	Der Administrator kann den Client automatisch bereitstellen und MobileIron Threat Defense auf ausgewählten Geräten aktivieren.	Benutzerakzeptanz 100 %	Ja	Ja
Erkennen von Bedrohungen	**Gerätesicherheitslücken** • Jailbreak • Root-Erkennung • Sicherheitslücken in der Betriebssystemversion • Mindest-Betriebssystemversion • Verschlüsselung deaktiviert • Passwort entfernt/deaktiviert • Dateisystemmanipulation • Nicht vertrauenswürdiges/verdächtiges Profil • Hochsetzung von Benutzerrechten **Netzwerk-Sicherheitslücken** • Man-in-the-Middle-Angriffe • Hotspots mit Schadsoftware • Ungesichertes WLAN • Bluetooth mit Schadsoftware • Unsaubere Zugangspunkte • Vorschaltseite **Anwendungs-Sicherheitslücken** • Hohes Datenschutzrisiko erkannt • Hohes Sicherheitsrisiko erkannt • Verdächtiges App-Verhalten • Mit Side-Loading installierte Apps	Erkennung bekannter und unbekannter Bedrohungen auf dem Gerät mit Algorithmen der künstlichen Intelligenz. Bessere Transparenz und Kontrolle von Geräten, Betriebssystem, Netzwerk sowie App-Sicherheitslücken und Bedrohungen.	Ja	Ja

App-Analyse	• **App-Transparenz:** Konfigurierbare Bestandsaufnahme der auf dem Gerät installierten Anwendungen
	  • Alle Anwendungen ([iOS])
	  • Verwaltete Anwendungen
	
	• **App-Analyse:** Optionale Offline-Analyse der Anwendungen. Die automatische Verknüpfung von App-Risiko und Geräteanalyse liefert Erkenntnisse in folgenden Bereichen:
	  • Inhalt: Malware
	  • Absicht: App-Verhalten
	  • Kontext: Domains, Zertifikate, gemeinsamer Code, Netzwerkkommunikation
	
	• **App-Intelligenz:** Definition von Sicherheitsrichtlinien, um Risiken zu verringern
	
	• **Berichte:** Drucken von Übersichten zur App-Sicherheit und zur Gefährdung der Privatsphäre
	
	• **Anwendungen hochladen:** Zur Analyse und Bewertung des Risikos
		Übersichten über die Apps, die auf dem Gerät installiert sind.
		
		Optional: Analyse mit detaillierten Berichten des Bedrohungsgrads, Erläuterung der Risiken und Konsequenzen.
			Ja	Ja

Benachrichtigung bei Bedrohungen	Der Administrator wählt die Bedrohungen aus, bei denen eine Benachrichtigung an den Gerätebenutzer gesendet werden soll, sobald die Bedrohung auf dem Server erkannt wurde. Benachrichtigungen können kundenspezifisch angepasst und in diversen Sprachen erstellt werden.	Konfigurierbare Benachrichtigung auf dem Gerät, wenn auf dem Gerät Bedrohungen erkannt werden.	Ja	Ja
Benachrichtigung bei lokalen Bedrohungen	Erstellung mehrerer lokaler Aktionskonfigurationen mit der aktuellen, automatisch importierten Bedrohungsliste. Das System benachrichtigt den Administrator, wenn eine neue Bedrohungsliste verfügbar ist und identifiziert Bedrohungen, die aus der Liste gelöscht wurden.	Der Administrator kontrolliert Umfang und Inhalt der Informationen über erkannte Bedrohungen, die den Gerätebenutzern angezeigt werden. Benachrichtigungen über Bedrohungen erfolgen in der Landessprache, die für das Gerät ausgewählt ist.	Ja	Ja

Maßnahmen zur Problembeseitigung	• Erstellung mehrerer lokaler Konfigurationen zur Problembeseitigung mit der automatisch importierten, aktuellen Bedrohungsliste.
	
	• Der Administrator wählt für jede nummerierte Bedrohung in der importierten Liste die Maßnahme der Plattform aus.
	
	• **Vom Server ausgelöste Compliance-Maßnahmen**
	  • Überwachen
	  • Warnung senden
	  • AppConnect und E-Mail sperren
	  • Quarantäne
	  • Selektive Löschung
	  • Mehrstufige Compliance (automatische und abgestufte Reaktion)
	
	• **Lokale Maßnahmen bei Android:**
	  • Quarantäne – Entfernung aller Konfigurationen
	  • Quarantäne – Entfernung aller Konfigurationen mit Ausnahme des WLAN, wenn nur WLAN vorhanden ist
	  • Entfernung aller Konfigurationen mit Ausnahme des WLAN
	  • Verwaltete Apps entfernen und Download sperren
	  • Bluetooth deaktivieren
	  • WLAN abschalten
	  • Gerät abschalten & löschen
	
	• **Lokale Maßnahmen bei iOS:**
	  • AppConnect-Apps sperren
	  • Netzwerk-Traffic umleiten
	
	• **Das System informiert den Administrator, sobald eine neue Bedrohungsliste verfügbar ist.**
		Die Compliance-Aktionen und die Benachrichtigungen über Bedrohungen erfolgen auf dem Gerät unabhängig davon, ob eine Internetverbindung vorhanden ist.
		
		Transformiert das Mobilgerät in einen Punkt zur Durchsetzung von Richtlinien, um die Erkennungszeit von Bedrohungen und Angriffen zu reduzieren und die „Kill Chain" für Angriffe über das Mobilgerät signifikant zu kürzen.
		
		Die lokale Compliance-Richtlinie ist mit der auf dem Gerät erkannten Liste von Bedrohungen immer aktuell. Dies spart Zeit und vermindert die Anzahl menschlicher Fehler.
		
		Es können mehrere lokale Konfigurationen zur Problembeseitigung erstellt und für verschiedene Benutzergruppen verwendet werden.
			Ja	Ja

Geräte auf Bedrohungen scannen	Laufend nach Bedrohungen scannen	Reduziert die Zeit zwischen Erkennung und Beseitigung mobiler Bedrohungen.	Ja	Ja
	Scan bei Geräteanmeldung ausführen	Optimiert den Datenschutz und verlängert die Batterienutzungsdauer.	Ja	Ja
Verwaltungskonsole	Integration der Cloud-zConsole in den Server für Unified Endpoint Management	Einfache Verwaltung von unternehmen- und mitarbeitereigenen Geräten	Ja	Ja

Bereitstellungsoptionen	Im eigenen Netzwerk oder als SaaS	Auswahl des Bereitstellungsmodells je nach den Anforderungen Ihres Unternehmens	Ja	Ja
Hosting-Standort	Server in verschiedenen Regionen der Welt	Auswahl der Standorte entsprechend den Anforderungen an den Datenschutz und die Latenzzeit	Ja	Ja
Datenschutzrichtlinien-kontrollen	Konfigurierbare Datenschutzrichtlinien zur Kontrolle der Offenlegung personenbezogener Daten	Einfache Compliance des Unternehmens mit der DSGVO, den bewährten Erfahrungen der Branche und den OEM-Anforderungen des Gerätes	Ja	Ja
Nachweislich für Masseneinsatz in Unternehmen geeignet	Einzelkunde mit > 250.000 Geräten	Bereitstellungserfahrungen vom Kleinbetrieb bis zum Großunternehmen	Ja	Ja
Landessprache	Übersetzt in 14 verschiedene Sprachen	Benutzerfreundlichkeit	Ja	Ja

Datenschutz

Ordnungsgemäß konfigurierte UEM-Sicherheits- und Sperrrichtlinien in Kombination mit MobileIron Threat Defense erlauben eine mehrstufige Sicherheitsstrategie mit automatischer Reaktion auf Bedrohungen, um die übertragenen bzw. gespeicherten personenbezogenen Daten eines Mobilgerätebenutzers zu schützen.

Support

In den Mitteilungen zum MobileIron Release finden Sie Informationen über weitere Produktspezifikationen.

Lizenzierung

Das Abo für MobileIron Threat Defense ist eine Ergänzung der Lizenz für Unified Endpoint Management und als Benutzer- oder Gerätelizenz erhältlich. Wenden Sie sich an Ihren Kundenbetreuer vor Ort bzw. Ihren Fachhändler, um zu erfahren, welche Preise für Ihr Unternehmen infrage kommen.