MobileIron

Fiche technique MobileIron Threat Defense

Présentation

La protection des appareils mobiles assurée par MobileIron Threat Defense est inégalée. Elle offre aux organisations la possibilité de détecter les cyberattaques au niveau d'un appareil, d'un réseau ou d'une application, et d'y remédier. À l'aide d'un agent intelligent unique, les organisations protègent leurs actifs des menaces connues et « zero-day » avec des algorithmes d'apprentissage automatique.

Threat Defense est déployé et activé sur les appareils mobiles gérés et non gérés de manière silencieuse, sans autre action de la part des utilisateurs, remportant ainsi leur adhésion. La correction des menaces s'effectue sur les appareils, même sans connexion Internet.

La protection contre les menaces ne perturbe pas la productivité des utilisateurs, et met les données et le réseau d'entreprise à l'abri des appareils mobiles piratés. Une fois activée sur un appareil, elle ne peut être ni supprimée ni désactivée par l'utilisateur.

Principaux avantages

Conçu pour les appareils mobiles, MobileIron Threat Defense utilise des algorithmes d'apprentissage automatique optimisés pour s'exécuter en continu sur les appareils et pour détecter les menaces même lorsque ces derniers ne sont pas connectés.

Facile à utiliser

Pour plus de facilité, la protection est intégrée à votre client MobileIron. Par ailleurs, aucune action des utilisateurs n'est requise pour l'activer.

Informations pertinentes

Bénéficiez d'une visibilité immédiate et permanente sur les menaces susceptibles d'affecter tous les appareils mobiles, ainsi que d'analyses détaillées sur les applications à risque.

Protection sur l'appareil

Profitez d'une détection et d'une correction inégalées des vulnérabilités connues et « zero-day » grâce aux algorithmes d'apprentissage automatique disponibles sur les appareils, sans qu'aucune connexion Internet soit nécessaire.

À propos de MobileIron

MobileIron propose un socle de sécurité pour le travail moderne. Pour obtenir davantage d'informations, veuillez vous rendre sur www.mobileiron.com.

MKT FR-FR v2.1

401 East Middlefield Road, Mountain View, CA 94043, États-Unis • globalsales@mobileiron.com • www.mobileiron.com • Tél. : +1877 819 3451 • Fax : +1650 919 8006

FONCTION-NALITÉ	DESCRIPTION	AVANTAGE	Système d'exploitation iOS	
Intégration UEM	Solution de protection contre les menaces intégrée à la gestion unifiée des terminaux.	Le service informatique ne gère qu'une seule application, pour des coûts d'exploitation moindres.	Oui	Oui
Déploiement automatisé	Le déploiement du client et l'activation de Threat Defense sur les appareils sélectionnés sont automatiques.	Adoption par 100 % des utilisateurs.	Oui	Oui
Détection des menaces	**Failles sur les appareils** • Jailbreak • Détection du root • Version de l'OS vulnérable • Version minimale de l'OS • Désactivation du chiffrement • Suppression/désactivation des mots de passe • Modification du système de fichiers • Profils suspects/non approuvés • Augmentation du niveau des privilèges **Failles sur le réseau** • Attaques de type « Man-in-the-Middle » • Points d'accès malveillants • Réseau Wi-Fi non sécurisé • Connexion Bluetooth malveillante • Points d'accès non autorisés • Portail captif **Failles au niveau des applications** • Risque élevé relatif à la confidentialité • Risque élevé relatif à la sécurité • Comportement suspect des applications • Chargement d'applications de sources inconnues	Détection de menaces connues et « zero-day » sur les appareils à l'aide d'algorithmes d'apprentissage automatique. Meilleure visibilité et meilleure connaissance des risques et menaces susceptibles d'affecter vos appareils, systèmes d'exploitation, réseaux et applications.	Oui	Oui

Analyse des applications	• **Visibilité sur les applications :** inventaire configurable des applications installées sur un appareil
	  • Toutes les applications (iOS)
	  • Applications gérées
	
	• **Analyse des applications :** analyse hors connexion et facultative des applications. Établit automatiquement un lien entre le risque lié à une application et l'analyse de l'appareil pour générer des données sur :
	  • Le contenu : logiciels malveillants
	  • L'intention : comportement de l'application
	  • Le contexte : les domaines, les certificats, le code partagé, les communications réseau
	
	• **Intelligence applicative :** définition de règles de sécurité pour réduire les risques
	
	• **Rapports :** création de rapports récapitulatifs sur les risques liés à la sécurité et à la confidentialité
	
	• **Téléchargement d'applications :** pour analyse et évaluation des risques
		Informations disponibles sur les applications installées sur un appareil.
		
		Fonction d'analyse optionnelle avec rapports détaillés sur l'évaluation des menaces, l'explication des risques et les implications.
			Oui	Oui

Notification en cas de menace	Sélection par l'administrateur des menaces pour lesquelles il souhaite que l'utilisateur d'un appareil reçoive une notification en cas de détection sur le serveur. Les notifications sont personnalisables et rédigeables dans plusieurs langues.	Configuration des notifications sur l'appareil envoyées en cas de détection de menaces sur ce dernier.	Oui	Oui
Notification en cas de menaces locales	Création de plusieurs configurations d'actions locales via l'importation automatique d'une liste des menaces actualisée. Le système informe l'administrateur de la disponibilité d'une liste des menaces mise à jour, et identifie les menaces qui ont été supprimées de la liste.	L'administrateur contrôle la quantité et le contenu des informations relatives aux menaces détectées fournies aux utilisateurs d'appareils. La langue dans laquelle s'affichent les notifications correspond à celle sélectionnée sur l'appareil.	Oui	Oui

Actions de correction	• Définition de plusieurs configurations d'actions de correction locales, par l'importation automatique de la liste des menaces actualisée.
	
	• L'administrateur choisit l'action à appliquer en fonction de la plateforme pour chacune des menaces répertoriées dans la liste.
	
	• **Actions de conformité initiées par le serveur**
	  • Surveillance
	  • Envoi d'une alerte
	  • Blocage d'AppConnect et de la messagerie
	  • Mise en quarantaine
	  • Effacement sélectif des données
	  • Conformité différenciée (réponse automatisée et graduelle)
	
	• **Actions locales sous Android :**
	  • Mise en quarantaine – suppression de toutes les configurations
	  • Mise en quarantaine – suppression de toutes les configurations, à l'exception de celle relative au Wi-Fi lorsque l'option Wi-Fi uniquement est sélectionnée
	  • Suppression de toutes les configurations, à l'exception de celle relative au Wi-Fi
	  • Suppression des applications gérées et blocage des téléchargements
	  • Désactivation du Bluetooth
	  • Déconnexion du réseau Wi-Fi
	  • Exclusion des appareils et effacement des données
	
	• **Actions locales sous iOS :**
	  • Blocage des applications AppConnect
	  • Déviation du trafic réseau vers un « puits » (sinkhole)
	
	• **L'administrateur est informé de la disponibilité d'une liste des menaces actualisée**
		Les actions de conformité et l'envoi de notifications en cas de détection de menaces sont effectués sur les appareils, avec ou sans connexion Internet.
		
		Transforme l'appareil mobile en point d'application des règles pour raccourcir les délais de détection des menaces et des attaques, et limiter sensiblement la « chaîne de frappe ».
		
		La règle de conformité locale est toujours à jour, grâce à la liste actualisée des menaces détectées sur l'appareil, pour un gain de temps accru et un risque d'erreur humaine limité.
		
		Définition de plusieurs configurations d'actions de correction locales, applicables à différents groupes d'utilisateurs.
			Oui	Oui

Recherche de menaces sur les appareils	Exécution d'analyses continues afin de détecter d'éventuelles menaces.	Réduction du temps qui s'écoule entre la détection d'une menace sur un appareil mobile et sa correction.	Oui	Oui
	Exécution d'une analyse à l'enregistrement d'un appareil.	Optimisation de la protection et de l'autonomie de la batterie.	Oui	Oui
Console de gestion	Intégration de la zConsole basée sur le cloud avec le serveur de gestion unifiée des terminaux.	Simplicité de gestion des appareils, qu'ils soient détenus par l'entreprise ou un employé.	Oui	Oui

Options de déploiement	Sur site, SaaS.	Choix du modèle de déploiement en fonction des besoins de votre entreprise.	Oui	Oui
Hébergement	Serveurs situés dans les principales régions du monde.	Choix de l'emplacement pour répondre aux exigences en matière de confidentialité des données et limiter la latence.	Oui	Oui
Contrôle des règles de confidentialité	Configuration de règles de confidentialité pour contrôler la divulgation des informations d'identification personnelles (PII).	Mise en conformité de l'entreprise avec le RGPD, les bonnes pratiques du secteur et les exigences des fabricants des appareils facilitée.	Oui	Oui
Évolutivité garantie	> 250 000 pour un seul client.	Déploiement pour les entreprises de toute taille.	Oui	Oui
Langues	Traduction dans 14 langues.	Simplicité d'utilisation.	Oui	Oui

Confidentialité

La configuration des règles de verrouillage et de sécurité UEM, combinée à MobileIron Threat Defense, fournit une sécurité renforcée et apporte une réponse automatisée contre les menaces, permettant de protéger les données personnelles au repos et en transit.

Compatibilité

Consultez les notes de version MobileIron pour plus d'informations sur les spécifications des produits.

Gestion des licences

L'abonnement MobileIron Threat Defense est une option en supplément de la licence de gestion unifiée des terminaux, que celle-ci s'applique par utilisateur ou par appareil. Pour en savoir plus sur les forfaits les mieux adaptés à votre entreprise, contactez votre représentant local ou votre revendeur.