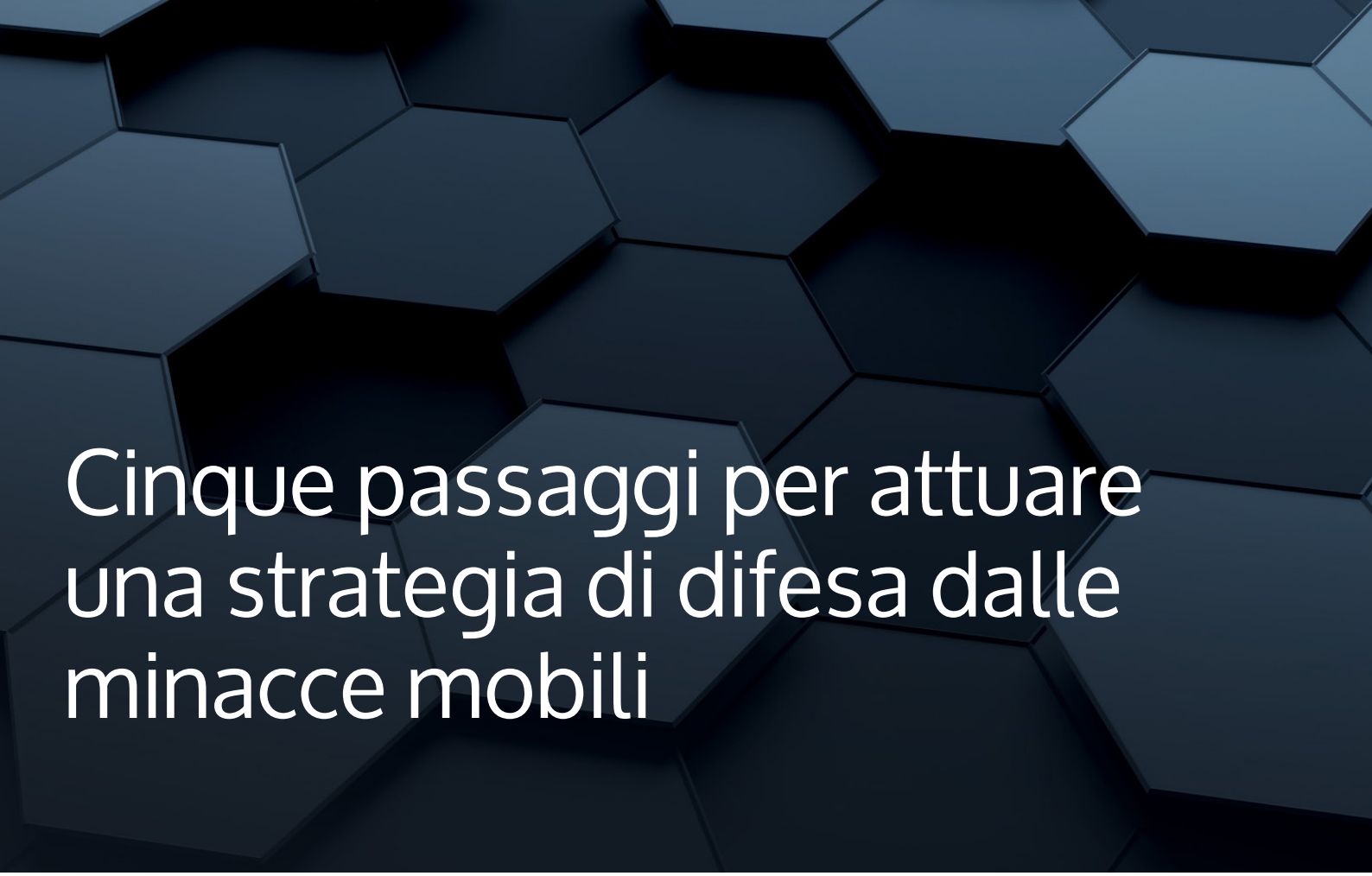


Cinque passaggi per attuare una strategia di difesa dalle minacce mobili

Proteggere il vostro business dalle minacce mobili è una corsa contro il tempo. State facendo il possibile per difendervi da un attacco?

I vostri dipendenti utilizzano mai le reti Wi-Fi gratuite disponibili all'interno di aeroporti, hotel o bar? E le porte USB? Come fate a sapere se i dispositivi in loro possesso sono immuni da attacchi Man-In-The-Middle (MITM) o dal tentativo di un malintenziato di rubare le loro credenziali aziendali? Avete adottato una strategia che vi consenta di riconoscere e bloccare questi tipi di attacchi?

Questa guida in cinque passaggi vi consente di mettere a punto una strategia basata sulle best practice in grado di fornire intelligenza immediatamente fruibile e protezione immediata dalle minacce mobili avanzate che prendono di mira la forza lavoro mobile. Scoprite come la difesa dalle minacce mobili può proteggere i vostri dispositivi, le app e i dati dai rischi per la sicurezza più recenti.

MobileIron

MKT IT-A4 v1.0

Una strategia Mobile Threat Defense (MTD) efficace rappresenta una corsa contro il tempo, poiché gli attacchi ai dispositivi mobili si stanno rapidamente intensificando e sta aumentando il loro livello di gravità. Poiché le organizzazioni che si celano dietro a questi exploit sono mosse dal desiderio di ingenti profitti, sono molto determinate e particolarmente abili nell'eseguire le loro attività. Un rapporto sulla sicurezza condotto nel 2017 dal Ponemon Institute stima che le aziende abbiano il 28% di probabilità di sperimentare una violazione ricorrente dei dati, che comporta la perdita di almeno 1.000 record contenenti informazioni personali su consumatori o clienti, informazioni di grande valore per i criminali informatici.[1] Le conseguenze di questo genere di attacco possono essere sconcertanti: oltre alla perdita dei dati o alla loro compromissione, una violazione dei dati sapientemente pubblicizzata può nuocere alle relazioni con i clienti, danneggiare la reputazione dell'azienda, causare la perdita di profitti, comportare multe e costi legali eccessivi, nonché sottrarre tempo e risorse preziosi per ripristinare la normalità.

Se non vi state adoperando al massimo per tutelare il vostro business da questo livello di rischio, ora è il momento di agire. Queste cinque best practice vi consentono di individuare i punti ciechi nell'ambito della sicurezza e di fornire protezione completa a tutti i dispositivi mobili che accedono alle app e ai dati aziendali, indipendentemente dal luogo di lavoro dei dipendenti e dalla rete che utilizzano.

Il panorama attuale delle minacce mobili

IL 75% DEGLI ATTACCHI
VIENE SFERRATO DA
MALINTENZIONATI ESTERNI

L'81% DELLE VIOLAZIONI CORRELATE ALLE INTRUSIONI
UTILIZZA PASSWORD RUBATE

IL 73% DELLE VIOLAZIONI
È CAUSATO DA MOTIVI FINANZIARI [2]

ICT Security Magazine, "2017 Data Breach Investigations Report, 10th Edition"

1 https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states

2 https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

MobileIron

Passaggio 1:
Attivare una difesa dalle minacce perfetta e invisibile

Alcune soluzioni di sicurezza mobile si affidano agli utenti finali per la protezione dei dispositivi mobili, un approccio all'MTD ritenuto insensato e inefficace. Queste soluzioni di "sicurezza basate sull'utente" richiedono che un dipendente mobile dell'azienda acceda all'app Store aziendale, scarichi il client e segua diversi passaggi per installare, attivare e mantenere l'app costantemente aggiornata. E quel è che peggio è che l'IT ha scarsissimo controllo sull'imposizione del client in quanto gli utenti possono semplicemente eliminare l'app o disattivarla mettendo a rischio i dati aziendali. Infatti, uno studio ha rivelato che oltre un terzo delle aziende non riesce a proteggere adeguatamente i propri dispositivi mobili per la mancanza di budget e delle risorse necessarie per implementare in modo uniforme la sicurezza avanzata all'interno dell'organizzazione.[3]

Le organizzazioni IT si affidano spesso agli utenti per attivare le app di sicurezza più recenti sui loro dispositivi. Ciononostante, se gli utenti non aggiornano correttamente i dispositivi, l'azienda può risultare vulnerabile agli attacchi nel caso in cui non tutti gli endpoint rispettino le policy di sicurezza. Non sorprendono quindi i risultati emersi da un rapporto di Dimensional Research condotto nel 2017, secondo cui "due terzi degli intervistati nel corso del sondaggio ha dichiarato di essere incerto sul fatto che la propria organizzazione possa difendersi da un attacco informatico mobile, mentre quasi tutti i professionisti nell'ambito della sicurezza ritengono che il numero di attacchi mobili sia destinato a crescere rapidamente."[4]

Per garantire la sicurezza completa e immediata su ogni dispositivo mobile che accede alle risorse aziendali, le organizzazioni devono smettere di fare affidamento sugli utenti per l'installazione degli aggiornamenti più recenti. Per implementare la sicurezza mobile avanzata senza problemi, Gartner consiglia alle organizzazioni di "integrare la soluzione MTD con lo strumento enterprise mobility management (EMM)."[5] Grazie a questo approccio, gli amministratori IT implementano la protezione e gli aggiornamenti della sicurezza direttamente nel dispositivo tramite l'EMM. Ciò significa che non è richiesto alcun intervento da parte dell'utente per scaricare e attivare gli ultimi aggiornamenti della sicurezza e che vengono supportate le informative sulla privacy. Una soluzione che integra l'EMM con l'MTD consente anche all'IT di focalizzare l'attenzione su priorità maggiormente strategiche e di ridurre le spese operative eliminando la necessità per gli amministratori di star dietro agli utenti per assicurarsi che i loro dispositivi siano conformi alle normative.

"Due terzi degli intervistati nel corso del sondaggio ha dichiarato di essere incerto sul fatto che la propria organizzazione possa difendersi da un attacco informatico mobile, mentre quasi tutti i professionisti nell'ambito della sicurezza ritengono che il numero di attacchi mobili sia destinato a crescere rapidamente."

— Dimensional Research,
"The Growing Threat of Mobile Security Breaches:
A Global Survey of Security Professionals"

3 https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
4 https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
5 https://www.gartner.com/doc/3789664/market-guide-mobile-threat-defense

Passaggio 2:
Visualizzare tutti i tipi di attacchi informatici

La mancanza di visibilità delle minacce mobili è una delle principali sfide per la sicurezza in ambito mobile che le aziende si trovano oggi ad affrontare. Infatti, oltre la metà (51%) delle aziende intervistate ha dichiarato di non sapere se sia mai stato scaricato del malware sui dispositivi mobili che i dipendenti usano per lavoro.[6] Alcune soluzioni di sicurezza mobile concorrono, di fatto, alla mancanza di visibilità, poiché si interessano unicamente alle minacce a livello di app. Eppure, non tutti gli attacchi informatici vengono sferrati nello stesso modo. Esistono diversi tipi di vettori di attacchi in grado di ignorare questo approccio ristretto impiegando altri mezzi. Perciò, le aziende non possono semplicemente focalizzarsi su un singolo livello; devono fornire sicurezza mobile completa e totalmente integrata per evitare attacchi a dispositivi, reti e applicazioni.

- **Attacchi a livello di dispositivo:** includono alcune delle più gravi minacce, poiché gli exploit messi a segno possono fornire ai mailintenzionati il controllo completo del dispositivo consentendo loro di rimuovere il contenuto crittografato. Gli attacchi a livello di dispositivo vengono spesso sferrati mediante i download gratuiti di app o attraverso un messaggio SMS che avvia il malware non appena l'utente lo apre.
- **Attacchi a livello di rete:** le reti pubbliche, benché utili e pratiche, possono anche fornire la rampa di accesso che veicola gli exploit direttamente ai dispositivi mobili. Ad esempio, da un punto di accesso non autorizzato della rete Wi-Fi gratuita di un hotel o di un bar è possibile sferrare un attacco Man-In-The-Middle (MITM) e intercettare le comunicazioni tra il dispositivo e la rete aziendale. L'autore dell'attacco può eseguire rapidamente la scansione del dispositivo alla ricerca delle vulnerabilità note che possono essere utilizzate per compromettere il dispositivo, acquisire i nomi utente, le password e i dati aziendali riservati utilizzandoli in seguito per accedere alle risorse aziendali.
- **Attacchi a livello di app:** di solito questi attacchi si verificano quando utenti ignari installano un'app da un app Store di terze parti. L'app contiene malware in grado di accedere alle autorizzazioni, eseguire l'exploit di un dispositivo e penetrare nelle reti interne per rubare i dati aziendali.

Le soluzioni che utilizzano algoritmi di apprendimento automatico sofisticati e rilevamento basato sul comportamento sul dispositivo mobile permettono alle organizzazioni di bloccare questi tipi di attacchi noti e sconosciuti (zero-day). Anziché focalizzarsi strettamente su un vettore di minaccia basato su una singola app, gli strumenti di apprendimento automatico sono in grado di riconoscere e bloccare immediatamente tutti i tipi di attività anomala, ad esempio una configurazione VPN non autorizzata o il download gratuito di un'app.

"Oltre la metà (51%) delle aziende intervistate ha dichiarato di non sapere se sia mai stato scaricato del malware sui dispositivi mobili che i dipendenti usano per lavoro."

— Zimperium,
"Mobile Security 2017 Spotlight Report"

6 http://go.zimperium.com/2017-mobile-security-report

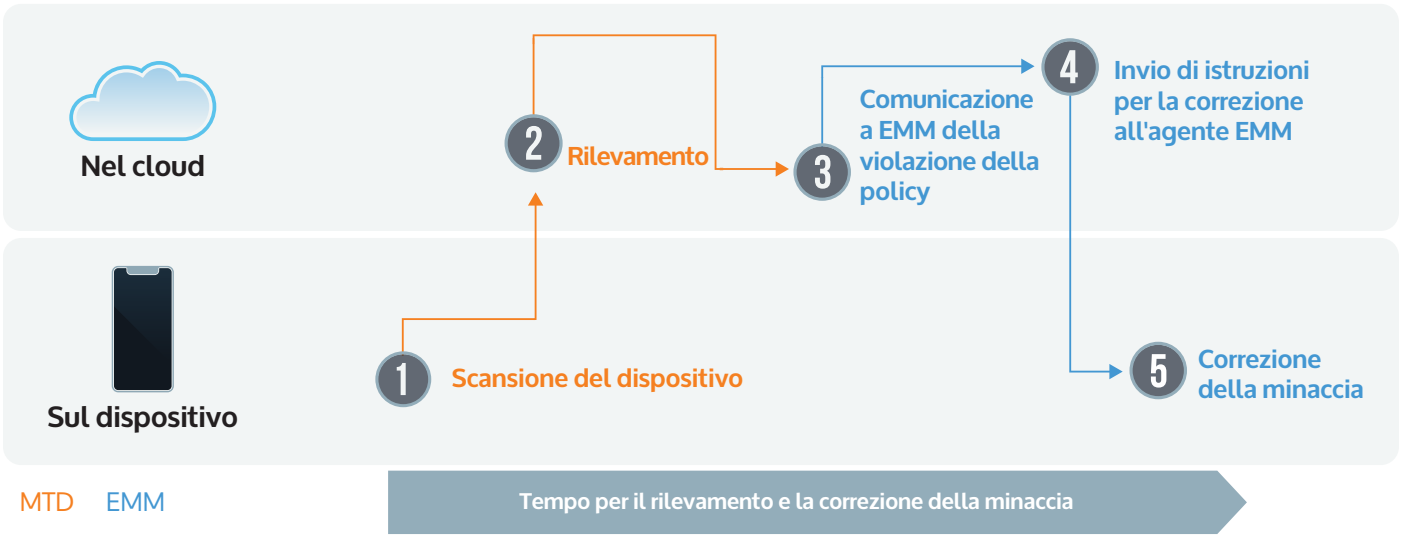
Passaggio 3:
Fornire informazioni immediatamente fruibili sulle minacce

Proprio come la mancanza di visibilità può creare punti ciechi per la sicurezza, anche una raffica costante di avvisi, che assegnano a tutte le minacce lo stesso livello di priorità, può causare il medesimo problema. Di conseguenza, negli amministratori della sicurezza mobile può insinuarsi il cosiddetto "affaticamento da avvisi", che rende difficile prendere decisioni rapide basate su informazioni aggiornate.

Per fornire informazioni sulle minacce fruibili nell'immediato, le soluzioni MTD devono includere un motore di analisi in grado di utilizzare algoritmi di apprendimento automatico che consentano di distinguere il comportamento normale da quello dannoso sul dispositivo stesso. Attraverso l'analisi di deviazioni minime rispetto alle statistiche del sistema operativo, della memoria, della CPU e di altri parametri di sistema del dispositivo mobile, l'apprendimento automatico è in grado di identificare in modo accurato non solo il tipo di attacco dannoso specifico, ma di fornire anche analisi forensi dettagliate associate al chi, che cosa, dove, quando e come di un attacco.

Le soluzioni di apprendimento automatico su dispositivo rilevano gli attacchi quando gli utenti non sono connessi alla rete o quando hanno a che fare con malware sconosciuto, nuove minacce o attacchi zero-day. Questo tipo di soluzione funziona più rapidamente rispetto alle soluzioni basate su cloud, dal momento che non è necessario effettuare il tunneling del traffico verso il cloud. Gli esperti di sicurezza mobile possono identificare rapidamente le minacce imminenti, assegnare loro una priorità e agire tempestivamente per impedire a un attacco grave di accedere alle risorse aziendali.

Rilevamento e correzione
Altre soluzioni MTD ed EMM



Passaggio 4:
Correggere le minacce dei dispositivi alla velocità della macchina

Poiché gli attacchi si verificano alla velocità della macchina, anche la sicurezza sui dispositivi deve rispondere con la stessa velocità. Di fatto, le soluzioni MTD basate solo sul cloud possono ritardare il rilevamento e la correzione delle minacce mobili sui dispositivi, poiché devono eseguire innanzitutto la scansione del dispositivo e inviare in seguito gli avvisi nel cloud prima di notificare alla soluzione EMM l'esistenza di una violazione della sicurezza. Ciò può comportare la perdita di tempo di risposta, che è fondamentale per contrastare un attacco potenzialmente devastante, ad esempio un attacco Man-In-The-Middle (MITM), che può prendere di mira un dispositivo mediante l'accesso a un Wi-Fi gratuito. In questo tipo di attacco il malintenzionato sferra un exploit che compromette il dispositivo mobile e che che gli conferisce un maggior controllo del dispositivo rispetto all'utente. Ad esempio, il malintenzionato può scaricare tutti i contatti dell'utente, rubare i messaggi e-mail e accedere come utente per inviare un'e-mail di phishing al CEO, con la possibilità di generare una violazione della sicurezza nell'intera azienda.

Una soluzione MTD su dispositivo consente di rispondere alle minacce alla velocità della macchina, poiché non richiede passaggi aggiuntivi per il rilevamento e la correzione delle minacce. Siccome l'intelligenza risiede nel dispositivo, quest'ultimo è in grado di rilevare immediatamente una violazione delle policy e bloccare la minaccia sul dispositivo interessato, inclusi gli attacchi Man-In-The-Middle. In una corsa contro il tempo, ciò consente di beneficiare del vantaggio decisivo sui malitenzionati e di evitare di incappare in problemi nel corso del tempo.

Rilevamento e correzione

La soluzione MobileIron Threat Defense

Passaggio 5:
Creare rapporti dettagliati per semplificare i requisiti di conformità

In qualsiasi azienda globale, la capacità di soddisfare le normative in materia di conformità impone alle organizzazioni di disporre di processi di audit e reporting chiari al fine di ottemperare a normative come, per citarne solo alcune, il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation), lo standard PCI DSS (Payment Card Industry Data Security Standard), le disposizioni dell'Health Insurance Portability and Accountability Act (HIPAA), nonché l'NDB (Notifiable Data Breaches) per la denuncia delle violazioni dei dati personali.

Nelle organizzazioni aziendali mobili è diventato ancora più difficile rispettare la conformità perché gli utenti non sono più legati ai computer desktop controllati dal reparto IT; infatti, gli utenti accedono ai dati e alle app aziendali da una varietà di dispositivi mobili personali e di proprietà dell'azienda su più reti. Secondo quanto evidenziato da un rapporto: "Una delle sfide insite nel rispetto della conformità al regolamento GDPR consiste nella protezione delle informazioni personali conservate su laptop e altri dispositivi mobili. Queste informazioni sono più difficili da monitorare e, di conseguenza, corrono un rischio maggiore di essere compromesse, poiché non si trovano dietro il firewall aziendale."[7]

La capacità di tenere traccia e gestire tutti i dispositivi e le app è fondamentale per soddisfare i requisiti di conformità, mantenendo un quadro chiaro delle minacce mobili generali e del comportamento associato ai rischi. Grazie alla capacità di generare con rapidità rapporti di audit, visualizzare registri delle minacce e tenere traccia delle cronologie di accesso e utilizzo dettagliate, gli amministratori sono in grado di individuare repentinamente potenziali vulnerabilità e garantire la conformità di utenti, dispositivi e app. In questo modo le aziende possono garantire il rispetto delle linee guida in materia di conformità e adoperarsi al massimo per proteggere il business dai rischi insiti nell'ambito mobile.

"Una delle sfide insite nel rispetto della conformità al regolamento GDPR consiste nella protezione delle informazioni personali conservate su laptop e altri dispositivi mobili. Queste informazioni sono più difficili da monitorare e, di conseguenza, corrono un rischio maggiore di essere compromesse, poiché non si trovano dietro il firewall aziendale."

GDPR: Report,
"GDPR Compliance for Mobile Workers," ottobre 2017

7 https://gdpr.report/news/2017/10/13/gdpr-compliance-mobile-workers

MobileIron THREAT DEFENSE

MobileIron Threat Defense: la soluzione di sicurezza mobile semplice e completa su dispositivo

MobileIron sa che i criminali informatici continuano a creare metodi più sofisticati per rubare con qualsiasi mezzo i vostri dati. Per questo motivo si impegna a innovare e a fornire costantemente nuove soluzioni in grado di aiutare i clienti a vincere la corsa contro il tempo, anticipando così le ultime minacce alla sicurezza mobile. Come parte di questo impegno, la soluzione MobileIron Threat Defense supporta i cinque passaggi fondamentali per l'implementazione della sicurezza mobile avanzata su dispositivo. La nostra soluzione fornisce una singola app integrata che offre diversi vantaggi chiave, tra cui:

- Una singola app di protezione dalle minacce completamente integrata con la soluzione EMM
- Possibilità di attivare o aggiornare la sicurezza sul dispositivo senza alcuna azione da parte dell'utente
- La sicurezza mobile avanzata blocca le minacce note e zero-day sui dispositivi iOS e Android senza bisogno di connessione Internet
- Gli algoritmi di apprendimento automatico rilevano e correggono immediatamente le minacce a dispositivi, reti e applicazioni (DNA) su dispositivo

Il risultato è la possibilità di beneficiare di sicurezza semplice e completa su dispositivo in grado di fornire intelligenza fruibile e protezione immediata dalle minacce a dispositivi, reti e app nell'intera forza lavoro mobile. Ciò consente di mettere in atto una strategia di sicurezza mobile moderna fondata sulla già comprovata affidabilità delle soluzioni EMM per fornire protezioni aggiuntive contro le minacce mobili. In questo modo potete occuparvi degli aspetti più importanti del vostro business, come salvaguardare la produttività dei dipendenti mobili e garantire che la vostra organizzazione mantenga un vantaggio competitivo, anche in materia di innovazione.

Per ulteriori informazioni sulla nostra soluzione per il rilevamento e la correzione delle minacce mobili completamente integrata, visitate la pagina www.mobileiron.com/threatdefense.

MobileIron

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