

MobileIron

Gestione unificata degli endpoint



Gestione unificata degli endpoint (UEM) per la protezione del lavoro moderno

Il lavoro moderno ha rivoluzionato le modalità di comunicazione, collaborazione e ottimizzazione della produttività all'interno dell'azienda. La gestione unificata degli endpoint (UEM) MobileIron consente ai dipendenti di sfruttare appieno i servizi cloud, le app, i computer desktop e i dispositivi mobili senza scendere a compromessi sulla sicurezza.

MobileIron UEM offre l'architettura attendibile e gestita necessaria per supportare il lavoro moderno

Supporto di un ambiente di lavoro con app attendibili. Consente il provisioning e la protezione delle app per cloud nell'endpoint, garantendo un'esperienza utente nativa semplificata. Separa i dati e le app aziendali dai dati e dalle app personali. Protegge le app per la produttività mobile che contengono soluzioni per la gestione di e-mail, contatti, calendario e attività nei dispositivi multi OS.

Accesso sicuro ai servizi cloud. Applica l'accesso condizionato in base alla postura dei dispositivi per proteggere servizi cloud quali Office 365, Box, G Suite e Salesforce dagli accessi non autorizzati.

Deployment di una piattaforma unificata per la sicurezza cloud e mobile. Consente di configurare e distribuire policy uniformi per le app in tutti gli endpoint e nel cloud. Le funzionalità VPN per-app consentono un accesso rapido alle risorse aziendali all'interno del firewall. La soluzione offre un browser mobile aziendale protetto, tramite il quale gli utenti possono accedere alle risorse Web interne in modo rapido e semplice.

Protezione e gestione



Dispositivi moderni:
Protezione delle e-mail
Configurazione automatica
Sicurezza basata su certificati
Cancellazione selettiva
Modalità Kiosk/App singola



App:
Applicazioni sicure
Vetrina virtuale di app aziendali
Enforcement dell'autenticazione utente
Isolamento/dismissione di app aziendali



Contenuti:
Allegati e-mail cifrati e visualizzabili solo nelle app autorizzate
Browser Web sicuri
Accesso, aggiunta di note e condivisione di documenti



Dispositivi monouso/modalità Kiosk:
Migliora la produttività limitando le app utilizzate su un dispositivo
Impedisce l'installazione di app dannose su un dispositivo
Evita i dati in eccesso limitando le app installate sul dispositivo

Casi di utilizzo principali

Sicurezza dei dispositivi

Configurazione e applicazione di policy uniformi per la sicurezza dei dati su computer desktop e dispositivi mobili con Android, iOS, macOS e Windows 10.

Sicurezza delle soluzioni e-mail

Accesso sicuro ai contatti, ai calendari e alle e-mail aziendali e garanzia di un'esperienza utente nativa su dispositivi mobili.

Sicurezza delle app e dei dati aziendali

Protezione dei dati aziendali sensibili (data-at-rest su dispositivi e data-in-motion nelle reti o nei servizi cloud).

Sicurezza dei contenuti mobili

Accesso sicuro e immediato ai repository dei contenuti e prevenzione delle perdite di dati causate dalla condivisione non autorizzata di file.

Dispositivi BYOD sicuri

Rispetto della privacy degli utenti nell'applicazione delle policy aziendali e mantenimento del controllo dei dati aziendali su computer desktop e dispositivi mobili personali.

Certificazioni e standard di sicurezza*

- Certificazione Common Criteria
- CSA STAR
- CSfC
- DISA STIG
- EU-US Privacy Shield
- Authority to Operate FedRAMP
- Convalida FIPS 140-2
- SOC 2 Type II

Informazioni su MobileIron

MobileIron fornisce alle aziende in tutto il mondo le basi sicure per trasformarsi in organizzazioni Mobile First. Per ulteriori informazioni, visitare www.mobileiron.com



401 East Middlefield Road • Mountain View, CA 94043
www.mobileiron.com • globalsales@mobileiron.com

Tel.: +1.877.819.3451
Fax: +1.650.919.8006

La gestione unificata degli endpoint (UEM) MobileIron consente ai dipendenti di accedere senza problemi ad app e dati aziendali tramite dispositivi mobili, desktop e servizi cloud sicuri, garantendo il controllo completo della privacy.



Bundle MobileIron UEM	Silver	Gold	Platinum
Opzioni di deployment UEM in locale e basate su cloud	✓	✓	✓
Sentry è un gateway in linea che si occupa di gestire, crittografare e rendere sicuro il traffico dati tra il dispositivo mobile e i sistemi aziendali back-end.	✓	✓	✓
Apps@Work è una vetrina virtuale di applicazioni aziendali che gestisce sia le app sviluppate internamente che le app aziendali di terze parti che possono essere distribuite agli utenti.	✓	✓	✓
AppConnect è un contenitore sicuro di app aziendali con VPN specifiche per le app abilitate AppConnect.		✓	✓
Email+ è un pacchetto sicuro di app per la produttività mobile che contiene soluzioni per la gestione di e-mail, contatti, calendario e attività per dispositivi iOS e Android.		✓	✓
Docs@Work consente di accedere, aggiungere note, condividere e visualizzare documenti in una vasta gamma di sistemi per la gestione di e-mail, contenuti on-premise e nel cloud.		✓	✓
Web@Work è un browser mobile aziendale sicuro che consente agli utenti finali di accedere alle risorse Web interne in modo rapido e semplice.		✓	✓
Gestione di desktop macOS per l'intero ciclo di vita: provisioning, configurazione, sicurezza, controllo, deployment di applicazioni, monitoraggio, conformità e fine del ciclo di vita.		✓	✓
Help@Work consente agli utenti di condividere il proprio schermo con un operatore dell'help desk per una risoluzione dei problemi più rapida ed efficiente.			✓
Tunnel offre funzionalità VPN per-app che consentono di autorizzare l'accesso di app specifiche alle risorse aziendali all'interno del firewall, senza intervento da parte dell'utente finale.			✓
MobileIron Monitor è una soluzione completa basata su dashboard che consente di gestire lo stato di tutti i componenti MobileIron UEM di importanza strategica.			✓
Le integrazioni di ServiceConnect consentono di semplificare i flussi di lavoro IT tramite l'app MobileIron per Splunk Enterprise e le integrazioni con ServiceNow.			✓
MobileIron Bridge consente di sfruttare gli script Group Policy Objects (GPO) esistenti per supportare la sicurezza granulare e la gestione dei PC con Windows 10.	SKU componente aggiuntivo, è necessario il bundle UEM MobileIron		
MobileIron Access offre un controllo dell'accesso sicuro e condizionato per servizi cloud quali Microsoft Office 365, Salesforce, G Suite, Box e tanti altri.	SKU componente aggiuntivo, è necessario il bundle UEM MobileIron		
MobileIron Threat Defense consente di proteggere i dati aziendali rilevando e risolvendo minacce note e zero-day su dispositivi mobili senza la necessità di connettività Internet, né di alcuna azione da parte dell'utente.	SKU componente aggiuntivo, è necessario il bundle UEM MobileIron		

Nota: informazioni soggette a modifiche senza preavviso.

MobileIron supporta l'azienda mobile moderna



Sfrutta la potenza di dispositivi, app e servizi cloud moderni e sicuri per consentire l'innovazione aziendale.

<https://www.mobileiron.com/en/solutions/enterprise-mobile-management-emm>



Offre controllo dell'accesso sicuro e condizionato per servizi cloud quali Microsoft Office 365, Salesforce, G Suite, Box e tanti altri.

www.mobileiron.com/en/access



Con una sola app, le aziende possono rilevare e risolvere minacce note e zero day su dispositivi mobili senza l'intervento dell'utente.

<https://www.mobileiron.com/en/threat-defense>



Usa gli script Group Policy Objects (GPO) esistenti per supportare la protezione granulare e la gestione dei PC con Windows 10.

www.mobileiron.com/en/bridge

* Per domande relative alla sicurezza e informazioni sulle differenze tra le certificazioni per deployment UEM nel cloud e on-premise, contattare il commerciale MobileIron.