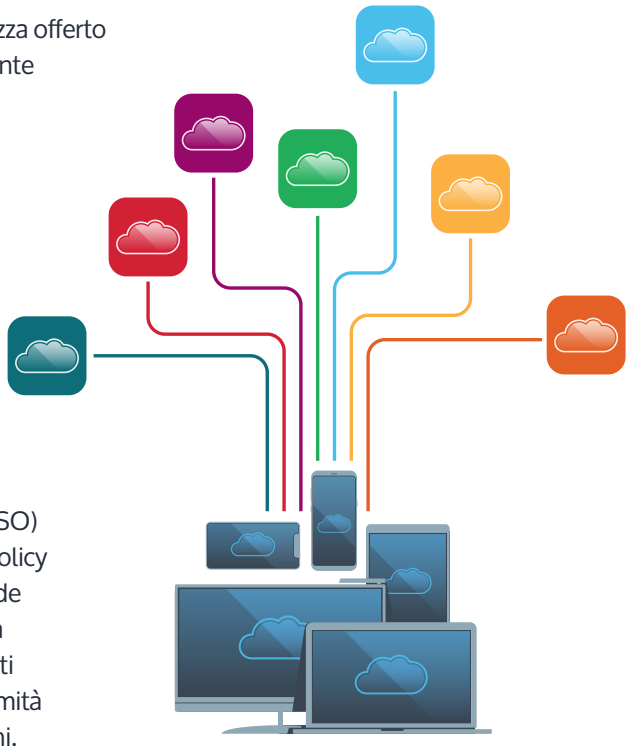
Sicurezza intuitiva e intelligente per il cloud aziendale

Proteggere le risorse cloud e mobili da accessi dannosi o non autorizzati è una delle sfide più impegnative che le aziende di oggi si trovano ad affrontare. Le funzioni di sicurezza che si affidano solo alle password non sono più all'altezza del compito. Nel 2018, infatti, il furto delle credenziali degli utenti è stata la prima causa delle violazioni dei dati aziendali.[1]

Nell'epoca dei computer, i dipendenti lavoravano entro un perimetro IT aziendale ben definito, dove l'impiego di password era sufficiente per stabilire l'attendibilità degli utenti. Nel mondo del cloud-mobile odierno, invece, il perimetro dell'azienda è scomparso e le informazioni aziendali risultano accessibili da più endpoint, app, servizi, reti e posizioni. Di fronte a un ambiente di accesso in continua evoluzione, le aziende devono adottare un nuovo approccio alla sicurezza, che sia in grado di:

- Verificare l'attendibilità degli utenti mediante l'autenticazione multi-fattore
- Mettere in correlazione l'attendibilità dell'utente con altri fattori, come l'endpoint, l'app, la rete e altro ancora
- Applicare policy adattive basate sul rischio e allineate all'ambiente degli utenti

Il nuovo framework di sicurezza offerto da MobileIron Access consente alle aziende di adottare le tecnologie cloud-mobile con la massima fiducia, aumentando la produttività degli utenti e riducendo il rischio di violazione dei dati.



Funzionalità come l'autenticazione multi-fattore (MFA), l'accesso Single Sign-On (SSO) semplificato e il motore di policy avanzato offrono alle aziende una piattaforma di sicurezza adatta a soddisfare i requisiti crescenti in termini di conformità e sicurezza delle informazioni.

Vantaggi principali
MobileIron Access è una soluzione di sicurezza basata su standard per gli ambienti cloud-mobile, che limita l'accesso delle informazioni aziendali agli utenti verificati su endpoint, app e servizi cloud autorizzati.

Semplicità
Le funzionalità offerte da Access, come la registrazione one-touch per l'autenticazione multi-fattore e l'accesso senza password per le app mobili, assicurano all'utente la migliore esperienza possibile.

Intelligenza
Le policy adattive e basate sul rischio tengono conto di vari fattori, come il tipo di endpoint, l'app, la rete, la posizione dell'utente e così via. Le funzioni di sicurezza sono allineate ai rischi nell'ambiente dell'utente e riducono le minacce rappresentate dalla violazione dei dati.

MobileIron

Informazioni su MobileIron
MobileIron è la base sicura per gli ambienti di lavoro moderni delle aziende globali di ogni dimensione. Per ulteriori informazioni su MobileIron Access, visita www.mobileiron.com/Access o rivolgiti al commerciale di MobileIron.

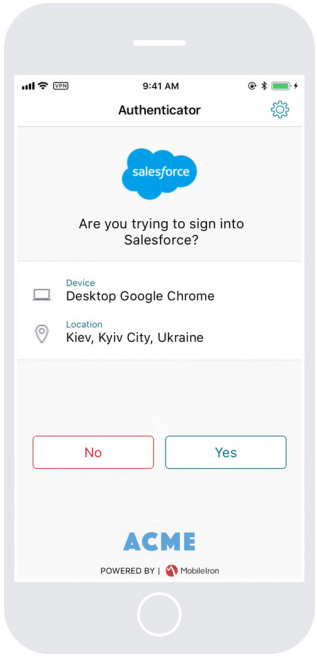
1 Verizon, 2018 Data Breach Investigations Report

Funzionalità

Autenticazione multi-fattore con MobileIron Authenticator

Un'app intuitiva per l'autenticazione multi-fattore, che sostituisce token complicati e costosi con una soluzione MFA sicura, semplice e conveniente per i dispositivi mobili.

- **Impostazione one-touch**
  L'impostazione e la configurazione vengono eseguite automaticamente tramite la piattaforma MobileIron. Per l'autenticazione one-touch, l'utente deve soltanto avviare l'app Authenticator. Al termine dell'attivazione, potrà verificare i tentativi di accesso sullo smartphone configurato.
- **Notifiche push**
  MobileIron Authenticator offre un metodo semplice e veloce per l'approvazione dei tentativi di accesso, che prevede l'invio di notifiche immediate sul telefono dell'utente.
- **Autenticazione adattiva**
  MobileIron Authenticator offre flussi di autenticazione intelligenti e compatibili con diversi tipi di feed, dalla postura degli endpoint a fattori quali app, rete e posizione dell'utente.



Autenticazione Single Sign-On nativa per gli endpoint moderni

L'autenticazione Single Sign-On nativa per i dispositivi mobili è una funzione ormai conosciuta da tutti gli utenti. Grazie ad essa è possibile collegarsi in sicurezza ai servizi aziendali senza prima effettuare l'autenticazione tramite un portale o un'app SSO diversa.

- **Accesso Single Sign-On intuitivo**
  Le policy adattive consentono agli utenti che si collegano tramite app ed endpoint autorizzati di eseguire l'autenticazione senza l'utilizzo di password.
- **Accesso Single Sign-On intelligente**
  L'accesso SSO basato sul contesto impedisce agli utenti di collegarsi ai servizi aziendali dalle app non gestite o dai servizi non autorizzati.

Motore affidabile per policy intelligenti

Consente di prendere decisioni intelligenti sul controllo degli accessi, tenendo conto non soltanto dell'identità dell'utente, ma anche di fattori quali il dispositivo, l'app, il servizio, la posizione dell'utente, la rete e così via.

- **Flussi di lavoro intuitivi per le attività di correzione**
  Procedure semplici e personalizzabili che consentono di risolvere autonomamente i problemi quando si utilizzano dispositivi non conformi. Non occorre perdere tempo e fatica per inviare ticket all'help desk.
- **Sicurezza basata su standard**
  Approccio basato su standard per la sicurezza di qualsiasi dispositivo, in grado di adattare il framework di sicurezza alle esigenze crescenti dell'azienda.