SONICWALL®

Garantire la sicurezza in un ambiente di lavoro mobile-first

Un approccio di sicurezza multilivello per garantire la gestione della sicurezza mobile

E-BOOK

Introduzione

Le aziende continuano a modificare e perfezionare le proprie strategie di gestione dei device mobili. Nonostante la comparsa di nuovi approcci come CYOD (Choose Your Own Device), COPE (Corporate-Owned, Personally Enabled) e COBO (Company Owned, Business Only), il BYOD (Bring Your Own Device) rimane tuttora molto diffuso e non accenna a diminuire in breve tempo.

La protezione dei dispositivi mobili richiede un approccio di sicurezza su più livelli per garantire una protezione completa contro varie minacce.

Rischi connessi ai dispositivi mobili

La mobilità e il BYOD comportano diversi rischi:

- Violazioni dei dati derivanti da smarrimento, furto o intrusione dei dispositivi
- Possibile diffusione di malware da un dispositivo infetto alla rete aziendale
- Problemi legali e normativi, in particolare se un dispositivo smarrito o rubato contiene dati aziendali sensibili
- Mancanza di conformità, che rende più difficile mantenere un ambiente IT sicuro

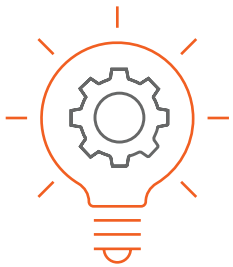
Alcune aziende hanno provato a combinare diverse tecnologie per proteggere i dispositivi e le reti in modo indipendente, ma questo approccio non è stato efficace.

Strumenti di sicurezza

Al giorno d'oggi, i responsabili IT possono implementare diversi strumenti di gestione della forza lavoro mobile e della sicurezza mobile per proteggere i dati e i dispositivi mobili:

- Gestione dei dispositivi mobili (MDM)
- Gestione delle applicazioni mobili (MAM)
- Gestione dei contenuti mobili (MCM)
- Gestione delle identità e degli accessi (IAM) mobile
- Rete privata virtuale (VPN) mobile

Ciascuno di questi strumenti presenta una serie di vantaggi e svantaggi.

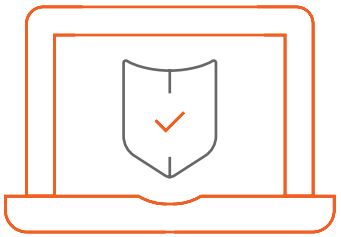


Gli strumenti di sicurezza dovrebbero migliorare la gestione del rischio e aiutare le organizzazioni a soddisfare i requisiti di conformità normativa.

Gestione dei dispositivi mobili

La gestione MDM (Mobile Device Management) consente agli amministratori IT di monitorare, controllare e proteggere i dispositivi che vengono utilizzati in azienda, indipendentemente dalla loro posizione. Il suo obiettivo principale è garantire la sicurezza dei dati sensibili archiviati e accessibili sui dispositivi mobili.

La gestione MDM offre la possibilità di cancellare i dati di un dispositivo in caso di smarrimento, ma richiede la gestione e l'amministrazione dei dispositivi personali da parte del reparto IT, che gli utenti potrebbero rifiutare per proteggere la propria privacy. I dati possono essere violati anche se vengono trasferiti ad altri dispositivi, perché MDM di solito crea policy a livello di utente e non di applicazioni. Inoltre, la gestione MDM non è in grado di bloccare la condivisione di informazioni tramite servizi cloud o altre applicazioni di terze parti.

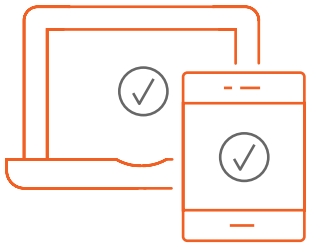


L'obiettivo principale della gestione MDM è garantire la sicurezza dei dati sensibili archiviati e accessibili sui dispositivi mobili.

Gestione delle applicazioni mobili

La gestione MAM (Mobile Application Management) viene utilizzata per gestire e proteggere le applicazioni mobili in uso all'interno di un'organizzazione. Fornisce protezione a livello di applicazioni piuttosto che a livello dei dispositivi o della rete. L'obiettivo principale della gestione MAM è garantire la sicurezza dei dati aziendali accessibili ed elaborati dalle applicazioni mobili.

La gestione MAM consente di impostare policy a livello di applicazione, ma non tutte le applicazioni possono essere gestite dalla MAM. Di conseguenza, potrebbe essere necessario lo sviluppo di applicazioni proprietarie e app personalizzate. Inoltre, la gestione MAM potrebbe non essere gradita agli utenti mobili che desiderano scegliere le applicazioni e i servizi da utilizzare.



L'obiettivo principale della gestione MAM è garantire la sicurezza dei dati aziendali accessibili ed elaborati dalle applicazioni mobili.

Gestione dei contenuti mobili

La gestione MCM (Mobile Content Management) può aiutare le aziende a soddisfare i requisiti di conformità, fornendo una piattaforma centralizzata per gestire e monitorare l'accesso ai documenti e garantendo che i dati sensibili non vengano compromessi. L'obiettivo principale della gestione MCM è consentire alle aziende di gestire e condividere in sicurezza i dati e i documenti aziendali sui dispositivi mobili, mantenendo il controllo sulle modalità di accesso e utilizzo delle informazioni.

La gestione MCM può essere costosa in termini di hardware, software e infrastruttura, senza contare i costi di supporto e manutenzione ordinaria. La conformità alle leggi sulla privacy dei dati e alle normative specifiche di settore può essere un processo complesso e continuativo.

L'obiettivo principale della gestione MCM è consentire alle aziende di gestire e condividere in sicurezza i dati e i documenti aziendali sui dispositivi mobili, mantenendo il controllo sulle modalità di accesso e utilizzo delle informazioni.

Gestione mobile delle identità e degli accessi

La gestione IAM (Identity and Access Management) mobile è un framework di sicurezza che consente agli utenti di accedere alle risorse aziendali in sicurezza dai propri dispositivi mobili, garantendo che questi dispositivi siano conformi alle policy e agli standard di sicurezza aziendali. L'obiettivo principale della gestione IAM mobile è fornire un accesso sicuro e conveniente alle risorse aziendali dai dispositivi mobili.

La gestione IAM mobile può peggiorare l'esperienza degli utenti e creare complessità e problemi di compatibilità. La necessità di digitare password complesse o di utilizzare l'autenticazione a più fattori (MFA) può essere un'esperienza frustrante per gli utenti. Inoltre, la gestione IAM mobile può essere complessa da implementare e gestire e potrebbe non essere compatibile con tutti i dispositivi o i sistemi operativi mobili, rendendo più difficile la gestione dell'ambiente mobile.

L'obiettivo principale della gestione IAM mobile è fornire un accesso sicuro e conveniente alle risorse aziendali dai dispositivi mobili.

Rete privata virtuale mobile

Una VPN (Virtual Private Network) mobile è una rete privata virtuale appositamente progettata per i dispositivi mobili. Come nel caso di una normale VPN, la connessione crea un tunnel sicuro tra se stessa e un server VPN e in genere utilizza un client per dispositivi mobili per facilitare questo processo. Uno dei vantaggi principali di una VPN mobile è la possibilità di utilizzare le reti Wi-Fi pubbliche in modo sicuro e protetto. L'obiettivo principale di una VPN mobile è fornire agli utenti una connessione internet sicura e privata e una maggiore libertà e flessibilità di accesso ai contenuti online.

Forse lo svantaggio maggiore dell'utilizzo di una VPN mobile (o di una VPN in generale) è il collo di bottiglia in termini di prestazioni sul server VPN. Poiché tutto il traffico viene instradato attraverso il server VPN, la connessione internet può rallentare a causa della crittografia e dell'elaborazione necessarie per instradare il traffico. Le prestazioni possono ulteriormente peggiorare sui dispositivi dotati di processori più lenti e meno RAM.

L'obiettivo principale di una VPN è fornire una connessione sicura e privata tra il dispositivo di un utente e Internet.

Il BYOD rimane molto popolare...

Un numero crescente di aziende sta implementando il BYOD semplicemente per il fatto che ormai tutti i dipendenti possiedono e utilizzano un dispositivo mobile.

L'83% delle aziende ha una policy BYOD di qualche tipo.*

*Statistiche di Zippia sul BYOD nel 2022

BYOD e protezione dei dati

Il BYOD per dispositivi mobili è diventato una realtà di fatto nell'ultimo decennio, e questa non è una novità. Al momento, gli ostacoli principali al BYOD sono le regole e le normative nel settore dei servizi finanziari. Sarà interessante vedere come questo settore risponderà ai requisiti per monitorare e archiviare *tutte* le comunicazioni elettroniche pertinenti (incluso il BYOD). Anche le leggi sul diritto alla privacy possono complicare il BYOD in questo settore.

A parte queste difficoltà nei settori altamente regolamentati, sembra che il BYOD sia ormai una realtà consolidata, almeno per il prossimo futuro. Le aziende devono valutare attentamente i potenziali benefici e rischi del BYOD e adottare policy e misure appropriate per ridurre i rischi e garantire un'esperienza positiva per gli utenti.

I dipendenti degli istituti finanziari devono rispettare rigorosi requisiti per il monitoraggio e l'archiviazione di *tutte* le comunicazioni elettroniche pertinenti.

Un approccio di sicurezza multilivello...

L'uso di un modello di sicurezza con diversi livelli di protezione dei dispositivi mobili è una soluzione ottimale. La sicurezza dovrebbe coprire come minimo la gestione dei dispositivi, delle identità e degli accessi e la protezione della rete, delle applicazioni e dei dati. Segue un elenco degli strumenti di sicurezza descritti in precedenza e il modo in cui soddisfano questi livelli di protezione:

- MDM → protegge i dispositivi e i dati sui dispositivi e contribuisce alla conformità
- MAM → protegge le applicazioni e i dati delle applicazioni e contribuisce alla conformità
- IAM → protegge l'accesso alle risorse digitali e contribuisce alla conformità
- VPN → protegge i dati e la privacy in rete
- MCM → protegge l'accesso e la condivisione di contenuti aziendali sensibili sui dispositivi mobili e contribuisce alla conformità

Una soluzione di sicurezza multilivello riduce i rischi del BYOD e della mobilità, offrendo agli utenti ciò che desiderano: poter utilizzare i propri dispositivi per accedere ai dati e alle applicazioni di cui hanno bisogno.

L'uso di un modello di sicurezza con diversi livelli di protezione dei dispositivi mobili è una soluzione ottimale.

Gestione della sicurezza mobile più semplice e veloce

Le soluzioni SonicWall forniscono ai responsabili IT il livello di gestione e sicurezza di cui hanno bisogno per soddisfare i requisiti di business aziendale. Gli utenti finali ottengono le funzionalità che desiderano e di cui hanno bisogno per svolgere il loro lavoro. I reparti IT non hanno più bisogno di acquistare, installare e gestire varie soluzioni mobili da diversi fornitori, con un conseguente risparmio di tempo e minori complessità. Le soluzioni Secure Mobile Access (SMA) e Enterprise Mobility Management di SonicWall consentono ai team IT di:

- Proteggere e gestire dispositivi endpoint, spazi di lavoro e container
- Fornire l'accesso sicuro ai dispositivi mobili
- Aumentare l'efficienza IT complessiva con potenti funzioni di controllo granulare degli accessi
- Ottimizzare la produttività dei lavoratori mobili, proteggendo al contempo le risorse dalle minacce

Per saperne di più ...

Contattaci per richiedere la consulenza di un esperto di sicurezza SonicWall.

Richiedi una versione di prova gratuita di Secure Mobile Access e provalo per 30 giorni.

Visita la nostra pagina web "Come proteggere l'accesso mobile ai dati e alle applicazioni aziendali".

SONICWALL

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Ebook-SMA-JK-8266