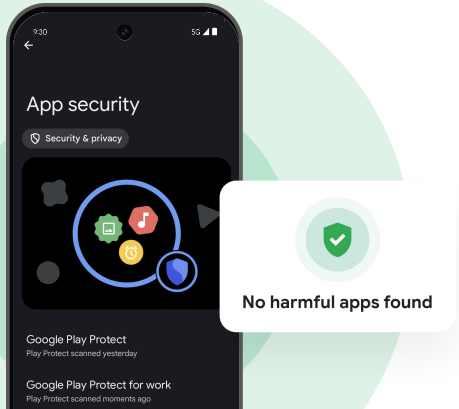
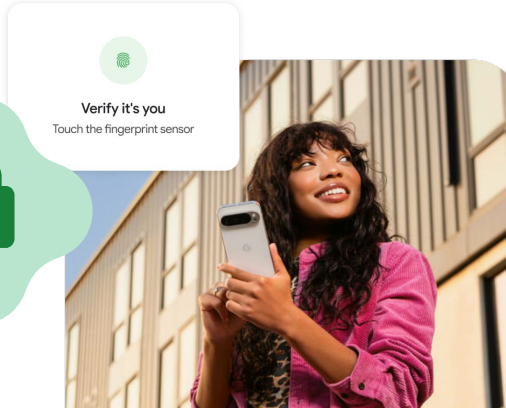
Android

Guida alla sicurezza per i dispositivi mobili per le PMI





Panoramica

L'implementazione di misure efficaci per garantire la sicurezza dei dati è fondamentale soprattutto per le piccole attività. Secondo Hiscox,[1] il 25% delle piccole imprese chiude i battenti dopo una violazione della sicurezza, che ha un costo medio di 200.000 $.

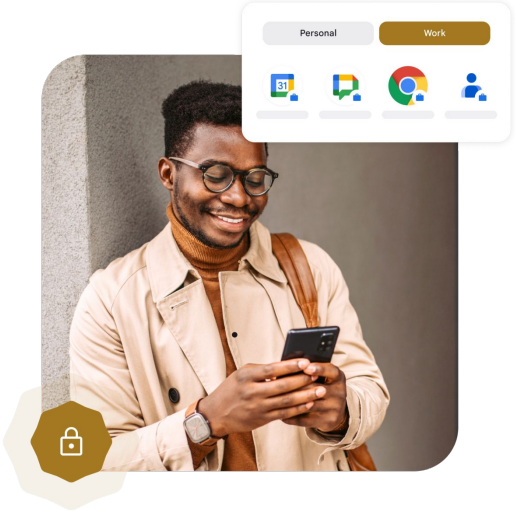
Nel mondo iperconnesso di oggi, smartphone e tablet sono uno strumento potente ma anche un potenziale rischio per la sicurezza, se non gestiti correttamente.

Una delle più grandi minacce per gli utenti di dispositivi mobili è il phishing: l'83% dei siti di phishing[2] prende infatti di mira i dispositivi mobili. I malintenzionati ora utilizzano l'AI per elaborare attacchi sofisticati, in grado di ingannare anche gli utenti più esperti.

Gestire l'intero ciclo di vita dei dispositivi aziendali e garantire la sicurezza e la privacy dei dati dei dipendenti e dell'azienda può sembrare un compito complesso, ma gli strumenti giusti possono rendere tutto più semplice.

Android offre misure di sicurezza semplici e discrete per contribuire a proteggere i dispositivi e i dati aziendali e difenderli dagli attacchi phishing. Questo aspetto è particolarmente importante per le attività che non possono contare su un'assistenza IT dedicata per la protezione e la gestione dei dispositivi.

In questa guida condividiamo le best practice per salvaguardare i tuoi dati aziendali e mettiamo in evidenza le caratteristiche che rendono Android una piattaforma solida e sicura.



[1] Hiscox Cyber Readiness Report
[2] Zimperium's 2024 Global Mobile Threat Report

Comprendere i modelli di registrazione dei dispositivi Android

Esistono tre direzioni o modelli specifici che le attività possono adottare per proteggere dispositivi e dati. Ogni modello aumenta il livello di controllo dei team IT su un dispositivo.

01

Il primo modello, che non utilizza tecnologie EMM (gestione della mobilità aziendale) o altre funzioni di gestione, è classificato come Avviato dall'utente. In questo modello, il team IT dell'azienda illustra agli utenti le best practice per configurare impostazioni di sicurezza e privacy specifiche sui propri dispositivi.

02

Nel secondo modello, Device Trust from Android Enterprise offre una soluzione basata su Zero Trust per una sicurezza avanzata. Questo approccio migliora la capacità dei fornitori di soluzioni attendibili di ispezionare lo stato di sicurezza di un dispositivo indipendentemente dal fatto che quest'ultimo sia gestito da una soluzione EMM. L'ampia gamma di soluzioni offerta include provider di identità (IdP), di soluzioni di difesa dalle minacce sui dispositivi mobili, di rilevamento e risposta a livello aziendale e di reti private virtuali (VPN). L'integrazione con Android Enterprise consente a queste soluzioni partner di verificare che vengano soddisfatti determinati criteri del dispositivo prima di concedere l'accesso alle risorse aziendali.

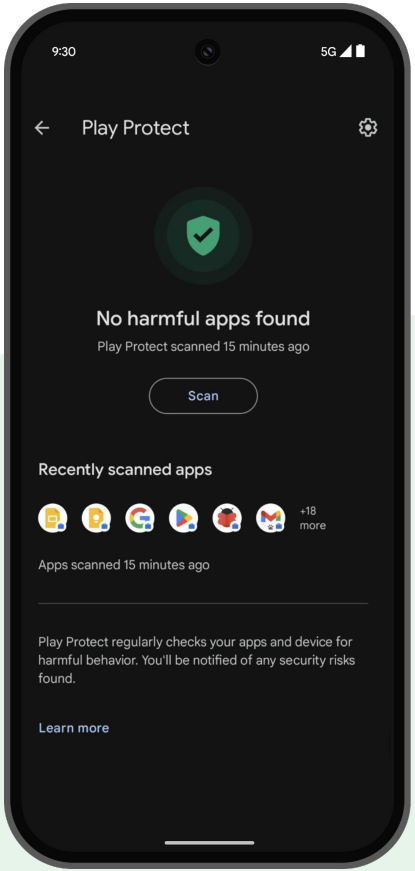
03

Il terzo modello si basa sui controlli di gestione della mobilità aziendale (EMM), che consentono alle organizzazioni di esercitare un maggiore controllo sui dispositivi degli utenti, siano essi di proprietà dell'azienda o parte di un programma BYOD (Bring your own device, Porta il tuo dispositivo). Nel caso dei dispositivi personali, l'azienda registra un profilo di lavoro, concedendo al team IT un controllo completo su tutti gli aspetti del profilo, preservando al contempo la privacy dell'utente nella sua area personale.

Android Enterprise offre diversi modelli di registrazione dei dispositivi per soddisfare le esigenze delle PMI

Ogni modello può essere integrato con gli altri per fornire alle PMI la massima flessibilità e possono anche essere utilizzati tutti insieme a seconda delle esigenze aziendali. Sfruttando le efficienti funzionalità di sicurezza di Android e implementando le seguenti best practice, la tua attività potrà operare con sicurezza nell'ambiente per dispositivi mobili.

L'impegno di Android nei progressi in materia di sicurezza, unito alla flessibilità e alla convenienza, lo rendono la scelta ottimale per le piccole e medie imprese.



Policy e impostazioni di sicurezza consigliate per i modelli di registrazione

Linee guida specifiche per ciascun modello: Avviato dall'utente, Device Trust from Android Enterprise ed EMM.

Ciascuno di questi modelli fornisce uno specifico livello di privacy dell'utente e di controllo aziendale in base alle tue esigenze.

01 Impostazioni di sicurezza per il modello Avviato dall'utente

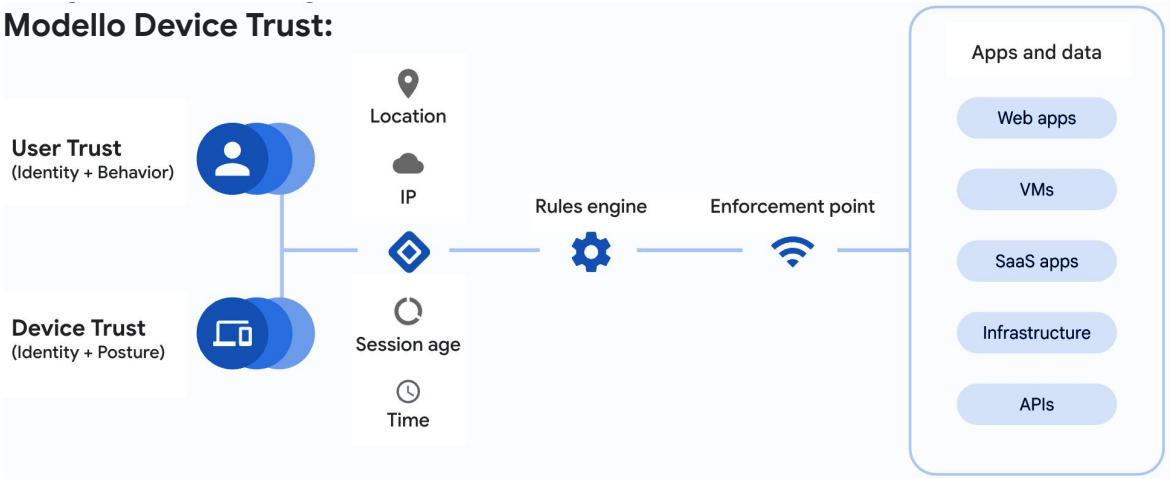
Il team IT fornirà al personale istruzioni su come e perché configurare manualmente le seguenti impostazioni sui loro dispositivi Android per contribuire a proteggere utenti e dati aziendali.

- Abilita Blocco per furto
- Abilita Blocco remoto
- Abilita Blocco dispositivo offline
- Abilita la Verifica dell'identità
- Abilita lo spazio privato
- Imposta un PIN o un passcode di almeno 6 caratteri non ripetuti
- Assicurati che Google Play Protect sia attivo
- Installa solo app dal Google Play Store

02 Modello Zero Trust

Oltre ai controlli e alle limitazioni disponibili con Device Trust from Android Enterprise, il team IT dovrebbe anche insegnare agli utenti a configurare e sfruttare tutte le funzionalità di sicurezza del modello Avviato dall'utente della sezione 1.

Modello Device Trust:



Scegli dall'elenco seguente i controlli che vuoi implementare prima di consentire l'accesso alle risorse aziendali. La scelta delle impostazioni dipenderà dai partner device trust (consulta la rispettiva documentazione).

02 Device Trust from Android Enterprise

Scegli dall'elenco seguente i controlli che vuoi implementare prima di consentire l'accesso alle risorse aziendali. La scelta delle impostazioni dipenderà dai partner Device Trust (consulta la rispettiva documentazione).

Indicatore	Descrizione
Modello o marca del dispositivo	Restituisce il modello e la marca del dispositivo.
Stato della gestione	Restituisce informazioni sulla gestione e sull'app di gestione.
Stato della rete	Restituisce informazioni su tutte le reti attive sul dispositivo.
Livello patch di sicurezza del dispositivo	Restituisce l'attuale livello patch di sicurezza del dispositivo (incluso il livello patch dell'aggiornamento di sistema di Play).
Livello patch di sicurezza pubblicato	Restituisce il livello patch di sicurezza pubblicato da Google per il componente aggiornabile corrispondente sul dispositivo.*
Stato della crittografia del disco	Indica se lo spazio sul dispositivo è criptato.
Versione del sistema operativo e aggiornamenti OTA in attesa	Restituisce la versione del sistema operativo del dispositivo e indica se è disponibile un aggiornamento del sistema operativo in attesa.
Blocco schermo e controllo qualità	Indica il livello di complessità dell'attuale blocco schermo dell'utente.
Stato di Play Protect	Indica se Google Play Protect è attivo.

03 Controlli attivati dalle policy EMM

Gli amministratori IT possono consultare la documentazione della soluzione EMM per scoprire come configurare questi insiemi minimi di policy per proteggere gli utenti. L'uso di una soluzione EMM consente al team IT di configurare i dispositivi come solo profilo di lavoro, COPE (Corporate-owned, personally enabled, Di proprietà aziendale, abilitati all'uso personale) o completamente gestiti. Sia il profilo di lavoro che la modalità COPE forniscono all'azienda un mezzo per controllare un profilo di lavoro, ma solo la modalità COPE offre un maggiore controllo sull'intero dispositivo. Ecco alcuni esempi di controlli di sicurezza da prendere in considerazione:

- Lunghezza minima della password: 6 caratteri
- Numero massimo di tentativi di sblocco del dispositivo: 10
- Abilita Google Play Integrity
- Disattiva gli screenshot
- Non consentire l'aggiunta di account nel profilo di lavoro
- Disattiva Opzioni sviluppatore
- Non consentire l'installazione da origini sconosciute
- Disattiva la funzionalità di copia e incolla tra i profili
- Non consentire Android Debug Bridge (ADB)
- Utilizza la versione gestita di Google Play con le liste consentite
- Chrome: impedisci la disattivazione di Navigazione sicura

Best practice per il deployment dei dispositivi Android nella tua attività

01 Insegna ai dipendenti ad abilitare le funzionalità di sicurezza integrate

Best practice

Proteggi i tuoi dati da ladri e accessi non autorizzati con funzionalità integrate aggiuntive progettate per salvaguardare le informazioni aziendali riservate, tra cui:

A

Attiva Blocco per furto, che utilizza l'AI, i sensori di movimento del dispositivo, il Wi-Fi e il Bluetooth per rilevare i movimenti assimilabili al furto e bloccare automaticamente il dispositivo.

B

Attiva e usa Blocco remoto.
In caso di smarrimento o furto del tuo dispositivo, puoi utilizzare Blocco remoto con un numero di telefono verificato per bloccare rapidamente lo schermo.

C

Attiva Blocco dispositivo offline. Dopo la disconnessione del dispositivo, la funzionalità Blocco dispositivo offline blocca automaticamente lo schermo del dispositivo per proteggere i tuoi dati. Ad esempio, se qualcuno ruba il tuo smartphone e disattiva internet per impedirti di trovarlo con Trova il mio dispositivo, lo smartphone si blocca dopo un breve periodo in cui risulta offline.

01 Insegna ai dipendenti ad abilitare le funzionalità di sicurezza integrate

Best practice

Proteggi i tuoi dati da ladri e accessi non autorizzati con funzionalità integrate aggiuntive progettate per salvaguardare le informazioni aziendali riservate, tra cui:

D

Attiva la Verifica dell'identità. Per verificare la tua identità, la Verifica dell'identità richiede dati biometrici e altre misure di salvaguardia. La tua identità viene verificata quando esegui azioni sensibili sul tuo dispositivo o apporti modifiche al tuo Account Google al di fuori dei luoghi attendibili.

E

Nascondi le app sensibili con lo spazio privato. Per salvaguardare le tue applicazioni private da accessi non autorizzati, Android offre la funzionalità "spazio privato". Ciò significa che sul dispositivo viene creata un'area nascosta separata in cui puoi organizzare le tue app personali. Anche se lo smartphone sbloccato finisce nelle mani sbagliate, le tue applicazioni sensibili nello spazio privato rimarranno protette.

F

Google ha inoltre integrato funzionalità antiphishing direttamente in Google Messaggi per proteggere gli utenti da tecniche di phishing sofisticate. Inoltre, sono disponibili nuove funzionalità come la protezione antispam e l'ID chiamante Android per migliorare ulteriormente la protezione degli utenti.

02 Usa la raccolta delle soluzioni Android Enterprise Recommended

Best practice

Crea un elenco di dispositivi approvati per l'uso sul lavoro dalla raccolta delle soluzioni Android Enterprise Recommended.

I dispositivi presenti nella nostra raccolta di soluzioni vengono sottoposti a rigorosi test di sicurezza e ricevono aggiornamenti tempestivi.

La convalida Android Enterprise Recommended garantisce che i dispositivi impiegati nella tua azienda dispongano di miglioramenti della sicurezza integrati e funzionalità ottimizzate per le esigenze aziendali.

03 Esegui il deployment di una soluzione di gestione dei dispositivi per il controllo centralizzato

Best practice

Utilizza una soluzione EMM per applicare le policy di sicurezza, cancellare i dati dei dispositivi o bloccarli da remoto e gestire le installazioni delle applicazioni. Per trovare un elenco di partner EMM convalidati e approvati, puoi visitare la raccolta di soluzioni EMM di Android Enterprise Recommended.

L'integrazione profonda di Android con le soluzioni EMM consente un controllo granulare e una gestione efficiente della sicurezza per aziende di qualsiasi dimensione.

04 Garantisci aggiornamenti della sicurezza tempestivi

Best practice

Utilizza le policy per i dispositivi Android Enterprise tramite una soluzione EMM per assicurarti che tutti i dispositivi siano aggiornati con le patch di sicurezza Android più recenti. Android Enterprise offre agli amministratori opzioni per applicare policy di aggiornamento del sistema operativo e delle applicazioni che soddisfino le esigenze aziendali.

Android si impegna a rilasciare aggiornamenti della sicurezza regolari ogni 30 giorni, in modo che l'ecosistema di produttori di dispositivi e operatori possa fornire gli aggiornamenti rapidamente. Inoltre, i dispositivi selezionati dalla raccolta delle soluzioni devono fornire aggiornamenti almeno ogni 90 giorni. I produttori di dispositivi, come Pixel e Samsung, ora offrono 7 anni di aggiornamenti del sistema operativo e della sicurezza. In questo modo, le potenziali vulnerabilità vengono corrette rapidamente con una patch.

05 Implementa l'autenticazione avanzata

Best practice

I controlli di Android Enterprise offrono la possibilità di impostare i requisiti per i passcode dei dispositivi. Tra questi ci sono PIN, sequenze e passcode, che possono essere abbinati allo Sblocco con l'Impronta o allo Sblocco con il Volto. Gli amministratori possono richiedere agli utenti di impostare requisiti specifici che soddisfino le esigenze dell'organizzazione. Assicurati che siano richieste almeno 6 cifre con caratteri non ripetuti, in conformità con le linee guida più recenti di NIST SP 800-53.

Il supporto dell'autenticazione biometrica di Android, unito all'archiviazione sicura dei token, offre agli utenti un'esperienza fluida e contribuisce a proteggere il dispositivo con un'autenticazione sicura e supportata da una crittografia hardware efficace.

06 Esegui il deployment delle applicazioni e gestiscile in sicurezza

Best practice

Consenti agli utenti di installare solo applicazioni provenienti dal Google Play Store e richiedi che Google Play Protect sia sempre attivo. L'utilizzo della versione gestita di Google Play consente agli amministratori di raccogliere un elenco di app approvate e impostare le autorizzazioni.

La versione gestita di Google Play impedisce il sideload di applicazioni non approvate, mentre Google Play Protect analizza attivamente tutte le applicazioni installate alla ricerca di malware.

07 Proteggi i dati in transito

Best practice

Utilizza le VPN per connessioni sicure ai servizi aziendali quando sei fuori dall'ufficio e assicurati che tutti i servizi utilizzino il protocollo HTTPS e che le connessioni Wi-Fi alla rete aziendale siano configurate correttamente.

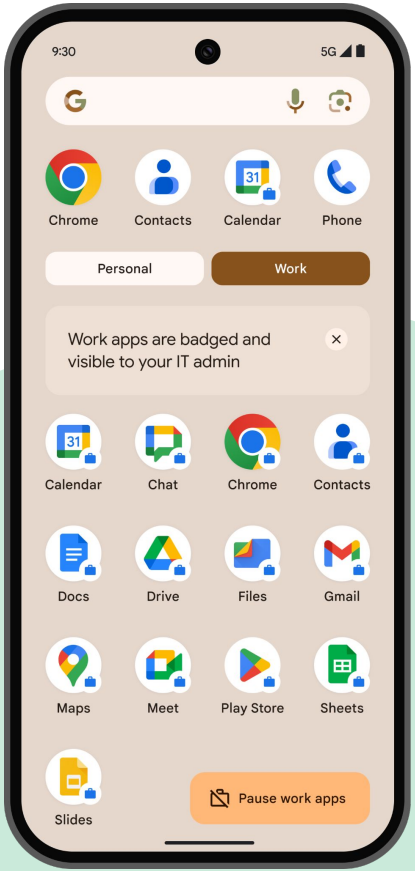
La crittografia integrata e il supporto delle VPN di Android contribuiscono a garantire la protezione dei tuoi dati, sia che siano archiviati sul dispositivo sia che vengano trasmessi tramite la rete.

08 Utilizza il profilo di lavoro Android

Best practice

Se i dipendenti utilizzano dispositivi personali (BYOD), gli amministratori devono implementare un profilo di lavoro per separare i dati aziendali e personali su un unico dispositivo.

Il profilo di lavoro Android, una funzionalità esclusiva di Android, crea un ambiente protetto e isolato per garantire la sicurezza dei dati aziendali e la privacy dei dati personali.



Concetti principali

Per ridurre al minimo le chiamate all'IT/help desk, è fondamentale formare gli utenti e offrire indicazioni chiare sulla configurazione di ciascuno dei tre modelli.

Consulta la raccolta delle soluzioni Android Enterprise per una selezione di partner e dispositivi approvati. Questa risorsa può aiutarti a scegliere i prodotti più adatti in base alle tue esigenze specifiche.

Dai la priorità all'implementazione una soluzione di sicurezza, anche se si tratta di un approccio di base. La protezione dei dispositivi di lavoro comporta costi per ogni modello. Scegli un modello che bilanci la sicurezza richiesta con le spese di implementazione e manutenzione.

Android

Scopri di più all'indirizzo

www.android.com/enterprise/security