Honeywell

THE POWER OF **CONNECTED**

TRANSIZIONE DEL SISTEMA OPERATIVO MOBILE

Approfondimenti e considerazioni

Introduzione

Nel corso degli ultimi anni è avvenuto un cambiamento nel panorama dei sistemi operativi mobili. La transizione dai precedenti sistemi operativi Windows® è a buon punto. Anche se persistono diverse scelte distinte sulla roadmap, i compromessi associati a ciascuna di esse sono diventati più chiari. Questo documento approfondirà l'argomento e fornirà al lettore una guida sulle soluzioni consigliate.

Indice

Storia dei sistemi operativi mobili

Per il sistema operativo Android open source, gli OEM di Google e terzi hanno iniziato a sviluppare estensioni che consentivano funzionalità di gestione dei dispositivi, offrivano maggiore controllo sulle azioni dell'utente e aggiungevano assistenza per le reti Wi-Fi industriali e funzionalità di scansione di codici a barre.

Dieci anni fa, i sistemi operativi per dispositivi mobili in ambito enterprise erano forniti da Microsoft. Windows CE e Windows Mobile (in seguito Windows Embedded Handheld) offrivano le caratteristiche e le funzionalità necessarie per la distribuzione aziendale, mentre un solido ecosistema di strumenti per sviluppatori e offerte di terze parti consentivano ai clienti di creare la soluzione adatta a utilizzare e gestire le proprie attività. Solo di recente Apple ha presentato il primo iPhone®. Google ha acquisito Android™ pochi anni prima e non aveva ancora avuto l'occasione di assistere alla commercializzazione di un telefono. Le altre opzioni disponibili all'epoca erano focalizzate soprattutto su impiegati professionali e non si sono rivelate adatte alle esigenze esclusive dell'ambiente enterprise specifico. Windows si è dimostrata una scelta valida ed è stato selezionato dalla maggioranza dei clienti che distribuivano dispositivi mobili rugged per le applicazioni operative.

La comparsa di funzionalità enterprise in iOS e Android è avvenuta solo diversi anni dopo e inizialmente è stato un processo piuttosto lento, mentre Apple e Google si concentravano sul mercato dei telefoni consumer in rapida crescita. Per il sistema operativo Android open source, gli OEM di Google e terzi hanno iniziato a sviluppare estensioni che consentivano funzionalità di gestione dei dispositivi, offrivano maggiore controllo sulle azioni dell'utente e aggiungevano supporto per le reti Wi-Fi industriali e funzionalità di scansione di codici a barre. Questo ha dato il via al primo ciclo di dispositivi Android mirati alle distribuzioni enterprise, a diversi round di miglioramenti e ha ampliato le offerte di prodotti perché i clienti hanno reagito positivamente alle interfacce touch intuitive e a un crescente ecosistema di app e sviluppatori. Tuttavia, questo approccio imprenditoriale ha anche dato origine alla frammentazione. Con l'aumentare del livello di modifica del sistema operativo base, più ci si distaccava dallo standard, rendendo più difficile l'esecuzione di applicazioni su prodotti di fornitori diversi, e meno probabile diventava la progressione rapida dei dispositivi notevolmente modificati alla versione successiva del sistema operativo base.

Apple ha risposto con i propri strumenti di gestione e miglioramenti enterprise per iOS, creando un vasto ecosistema di sviluppatori. Tuttavia, il sistema chiuso di Apple continua ad avere limiti in termini di controllo degli aggiornamenti e gestione di alcune funzionalità dei dispositivi. Poiché i dispositivi hardware sono limitati a telefoni e tablet consumer, iOS è una soluzione adatta ai casi di utilizzo che richiedono un dispositivo mobile rinforzato solo tramite l'aggiunta di casi esterni.

Sistemi operativi precedenti

Poiché le date di fine supporto per i sistemi operativi precedenti si avvicinano, i clienti devono prendere decisioni e pianificare le prossime operazioni, perché lo sviluppo delle applicazioni può richiedere tempo e impegno considerevoli.

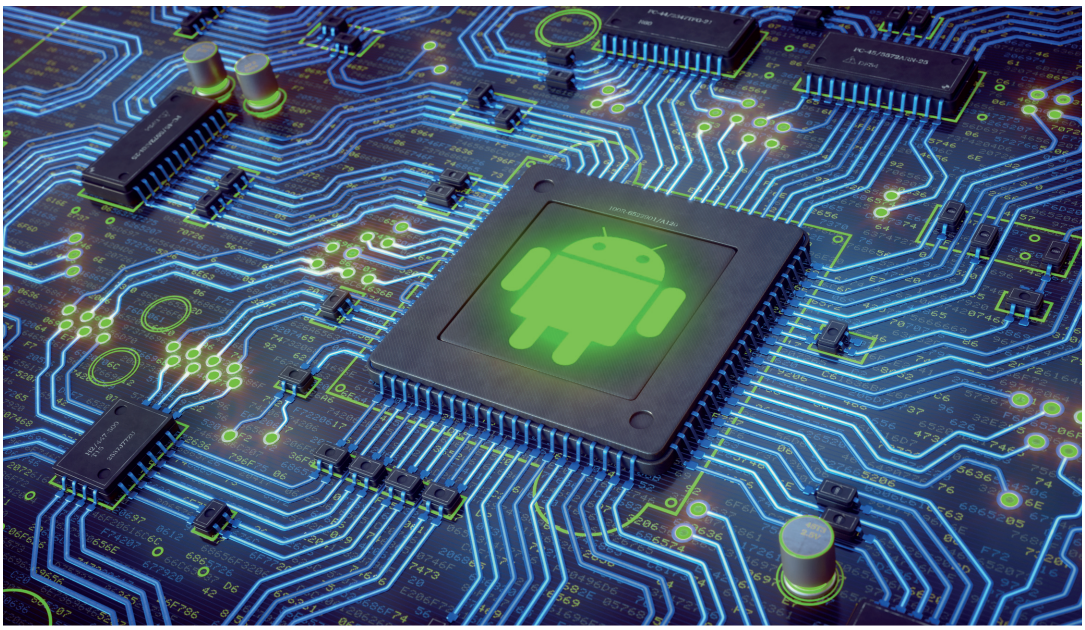
I clienti che eseguono attualmente applicazioni che richiedono un sistema operativo Microsoft precedente (Windows CE 6 o Windows Mobile/Windows Embedded Handheld 6.5) dovranno affrontare a breve il problema della fine del supporto per le loro piattaforme. Il supporto Mainstream, che include aggiornamenti regolari, è terminato per entrambi i sistemi precedenti. Il supporto esteso Microsoft (correzioni rapide per la protezione) terminerà per Windows CE 6 all'inizio del 2018 e per Windows Embedded Handheld 6.5 all'inizio del 2020. Dopo tali periodi, i fornitori non potranno più fornire patch in caso di vulnerabilità o errore rilevati nel codice Microsoft. Per questo e altri motivi, molti clienti hanno iniziato a pianificare una transizione a nuove applicazioni eseguibili in un sistema operativo moderno.

Poiché le date di fine supporto per i sistemi operativi precedenti si avvicinano, i clienti devono prendere decisioni e pianificare le prossime operazioni, perché lo sviluppo delle applicazioni può richiedere tempo e impegno considerevoli. Un modo per avere più tempo per prendere la giusta decisione è selezionare un hardware in grado di supportare più sistemi operativi. I computer portatili Honeywell delle serie CN75 e CK75, insieme al computer portatile Honeywell CN51, offrono la scelta di Windows Embedded Handheld o Android. Inoltre, i clienti che acquistano Windows Embedded Handheld possono convertire i propri dispositivi in Android in futuro. Ciò consente di continuare a eseguire le applicazioni precedenti esistenti fino a quando l'organizzazione non è pronta a passare ad Android, momento in cui sarà eseguita una semplice conversione del software sul campo. È richiesto un minimo investimento software e non saranno necessari costi per l'hardware.

La vasta presenza sul mercato di Android supporta un'ampia gamma di OEM e fattori di forma hardware, pertanto sarà più probabile trovare un dispositivo che soddisfi i requisiti di costi e utilizzo del cliente, inclusi i dispositivi che offrono tastiere numeriche fisiche integrate.

Android Enterprise Evolution

Google ha continuato a investire massicciamente nelle funzionalità enterprise in ciascuna delle ultime tre versioni, modificando il nome di Android for Work in Android Enterprise.



Prima di 4.0 Ice Cream Sandwich, Android offriva poco nel settore delle funzionalità enterprise. Il sistema operativo focalizzato sul consumatore è stato ampliato tramite estensioni OEM e da software di terzi per poterlo controllare e gestire in ambiente enterprise. Le funzionalità enterprise hanno iniziato a comparire gradualmente nelle versioni 4.2 Jelly Bean e 4.4 KitKat e hanno raggiunto l'apice con l'introduzione di Android for Work in 5.0 Lollipop. Android for Work ha fornito un set esteso di API di gestione e un sistema contenitore per separare e gestire indipendentemente app e dati di lavoro e personali.

Google ha continuato a investire massicciamente nelle funzionalità enterprise in ciascuna delle ultime tre versioni, modificando il nome di Android for Work in Android Enterprise. Le funzionalità aggiunte includono il provisioning in blocco per velocizzare la configurazione dei dispositivi, la modalità Proprietario dispositivo per consentire dispositivi totalmente gestiti a livello corporate, always-on VPN e crittografia abilitata per impostazione predefinita per proteggere i dati personali e corporate.

I sistemi operativi mobili noti come Android consentono alle società di accedere a un vasto ecosistema di applicazioni, strumenti di sviluppo e risorse, ma implicano anche rischi per la sicurezza che devono essere affrontati e mitigati. Android ha sviluppato costantemente il suo approccio alla sicurezza. Con la crescita della sua quota di mercato, Android è diventato un bersaglio di exploit e attacchi malware. Google ha risposto aumentando le protezioni per impedire l'introduzione di PHA (Potentially Harmful App), nonché implementando difese all'interno del SO che limitano la compromissione del sistema in caso di installazione di una PHA. Alcune di queste protezioni sono illustrate di seguito. Le informazioni dettagliate sono disponibili nel report Android Security 2016 Year in Review di Google disponibile qui:

https://source.android.com/security/reports/Google_Android_Security_2016_Report_Final.pdf

L'offerta Honeywell

Il team di sicurezza informatica monitora più fonti di informazioni per rilevare potenziali problemi di sicurezza del sistema il più presto possibile (generalmente ben prima dei principali mezzi di comunicazione) e ha implementato un protocollo di escalation che mobilita le risorse di tutta società su base prioritaria per risolvere tali problemi.

Honeywell è fortemente impegnata nel settore della sicurezza informatica. Le nostre attività globali includono soluzioni aerospaziali e di processo che richiedono un livello di sicurezza molto elevato in tutti gli aspetti delle operazioni. Una task force di sicurezza informatica a livello corporate stabilisce e mantiene politiche e standard di sicurezza, tra cui procedure di prova utilizzate in fase di sviluppo dei prodotti che individuano specificatamente problemi software che potrebbero rendere i sistemi più vulnerabili agli exploit. Questo approccio elimina le potenziali vulnerabilità addirittura prima che i prodotti siano rilasciati.

Il team di sicurezza informatica monitora più fonti di informazioni per rilevare potenziali problemi di sicurezza del sistema il più presto possibile (generalmente ben prima dei principali mezzi di comunicazione) e ha implementato un protocollo di escalation che mobilita le risorse di tutta società su base prioritaria per risolvere tali problemi. Una volta individuata una vulnerabilità di Android e pubblicata un'azione correttiva da parte di Google, gli esperti in sicurezza Android di Honeywell implementano la soluzione e la forniscono ai clienti. La distribuzione diretta di patch e aggiornamenti consente ad Honeywell di ridurre il tempo di risposta rispetto agli OEM che devono passare attraverso canali secondari per fornire i propri aggiornamenti.

Per tutti i prodotti Honeywell sono pubblicati manuali sulla sicurezza che guidano i clienti nell'implementazione di best practice per proteggere il proprio ambiente e i dispositivi. Viene fornita assistenza per la configurazione delle impostazioni dei dispositivi, delle impostazioni di rete e per la manutenzione di un ambiente IT protetto. Queste misure preventive sono volte a ridurre le vie attraverso le quali le minacce possono attaccare l'ambiente del cliente.

Molti clienti enterprise sceglieranno di limitare ulteriormente gli utenti finali "bloccando" il dispositivo tramite l'utilizzo dell'agente MDM (Mobile Device Management) o di un'app come Honeywell Enterprise Launcher. Questi strumenti controllano l'accesso dell'utente alle risorse del sistema e possono limitare il sistema a eseguire solo determinate app. Eliminando la possibilità dell'utente di installare o eseguire app non autorizzate si rende il sistema meno vulnerabile a exploit della sicurezza causati da azioni dell'utente. Honeywell offre una libreria di API per toolkit enterprise che consente ai clienti di istituire white list o black list di applicazioni, controllare la disponibilità di un'ampia gamma di funzionalità del dispositivo e controllare gli indirizzi IP accessibili tramite firewall. Honeywell Launcher sostituisce la schermata iniziale Android

standard con un'esperienza a tutto schermo che consente all'utente di visualizzare ed eseguire solo le app necessarie allo svolgimento del proprio lavoro. Honeywell offre anche un browser enterprise che consente il rendering delle pagine Web tramite comandi Android standard, ma controlla i siti che gli utenti sono autorizzati ad aprire. Limitando le operazioni che l'utente può eseguire con il dispositivo, il supporto IT diventa più facile e le opportunità di introduzione di malware nel sistema si riducono drasticamente.

Un altro aspetto importante della sicurezza è il mantenimento di un sistema aggiornato. I ricercatori scoprono costantemente e riferiscono con responsabilità le vulnerabilità della base di codici Android che potrebbero potenzialmente essere oggetto di exploit dannosi. Google offre anche un programma di ricompense per incoraggiare i ricercatori a trovare e riferire potenziali problemi. Google e i fornitori di chipset come Qualcomm forniscono regolarmente agli OEM patch per la sicurezza da incorporare nelle proprie build software. Honeywell aggiorna le proprie immagini di sistema Android con una cadenza regolare di 60 giorni, con patch per exploit estremamente critici disponibili in solo pochi giorni (secondo necessità). Le patch vengono fornite come aggiornamenti incrementali alle immagini di riferimento, riducendo al minimo le dimensioni del pacchetto di aggiornamento per agevolare la distribuzione sulla rete del cliente. Diversamente dagli OEM consumer, i pacchetti Honeywell sono scaricabili da un portale Web per consentire il test di convalida cliente prima della distribuzione su larga scala. È disponibile una sottoscrizione alle notifiche email che consente ai clienti di ricevere avvisi non appena vengono pubblicati nuovi aggiornamenti.

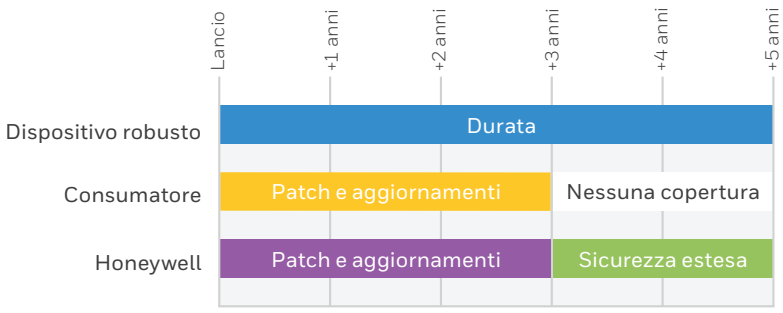
Gestione del ciclo di vita Android

Honeywell offre un programma per fornire patch per vulnerabilità della sicurezza importanti applicabile al sistema operativo supportato su base periodica per più di 2 anni dal termine del supporto della patch di sicurezza di Google.

I clienti che utilizzano soluzioni per computer portatili nell'ambiente enterprise rugged prevedono un ciclo di utilizzo più lungo rispetto ai consumatori. Mentre gli smartphone nei casi di utilizzo consumer durano generalmente 2-3 anni, l'aspettativa enterprise è una durata dei sistemi di almeno 3-5 anni. Storicamente, i sistemi operativi utilizzati nei computer portatili rugged avevano un ciclo di vita corrispondente ai casi di utilizzo enterprise. Windows CE e Windows Embedded Handheld sono supportati da Microsoft per 10 anni dopo l'introduzione iniziale.

Anche se Android è stato ampliato da Google con svariate nuove funzionalità enterprise in ogni nuova release, il supporto esteso non è tra queste. Le principali versioni di Android (o "versioni dessert") vengono rilasciate all'incirca su base annuale e sono generalmente supportate da pach di sicurezza di Google e fornitori di chipset per i 3 anni successivi. Ciò crea un divario nella copertura del supporto relativamente alle aspettative enterprise. La selezione di chipset OEM supportati per release dessert successive contribuirà a prolungare i tempi, ma in definitiva la politica di supporto di Google termina prima delle aspettative dei clienti enterprise.

Honeywell offre un programma per fornire patch per vulnerabilità della sicurezza importanti applicabile al sistema operativo supportato su base periodica per più di 2 anni dal termine del supporto della patch di sicurezza di Google.



- La tempistica di consegna ai clienti sarà trimestrale o inferiore se non vengono riferite patch importanti applicabili alla versione del sistema operativo supportato. Le patch applicabili saranno generalmente consegnate entro 90 giorni dalla divulgazione pubblica, ad eccezione di possibili minacce imminenti.
- Si presuppone che i clienti che utilizzano questo servizio abbiano applicato tutte le patch rilasciate in precedenza al fine di applicare quelle più recenti. In altre parole, le patch sono cumulative relativamente all'ultima release di manutenzione del SO. Non è possibile applicare singolarmente patch specifiche.
- Le patch di sicurezza saranno testate in base alle procedure di test standard di Honeywell applicabili a tutte le release software. È responsabilità del cliente testare in modo soddisfacente eventuali aggiornamenti software ricevuti da Honeywell prima di eseguire un aggiornamento nel proprio ambiente.
- I clienti riceveranno tali vantaggi conformemente ai termini di un contratto di servizio, indipendente o incorporato in un altro tipo di accordo di servizio. I clienti senza contratto non riceveranno patch di sicurezza al termine del supporto patch di sicurezza di Google.

Questo programma sarà disponibile sui dispositivi Honeywell che eseguono Android 6.0 Marshmallow e versioni successive, allo scadere del supporto patch di sicurezza di Google.

Conclusione e consigli

Android è un sistema operativo sicuro che utilizza tecniche di mitigazione degli exploit e isolamento delle applicazioni per offrire all'utente un livello elevato di sicurezza. L'implementazione di tecniche di blocco tramite un MDM o Honeywell Enterprise Launcher può ridurre ulteriormente il rischio di intrusione di malware limitando le operazioni eseguibili dall'utente e le app che possono essere eseguite sul sistema.

I prodotti Honeywell sono progettati fin dall'inizio per soddisfare i rigorosi standard di sicurezza di Honeywell. La sicurezza viene valutata in tutto il processo di sviluppo, identificando e mitigando le vulnerabilità addirittura prima del rilascio dei prodotti. La formazione dei clienti e il monitoraggio costante delle vulnerabilità della sicurezza e degli exploit, con processi definiti per risolvere i problemi rilevati, proteggono ulteriormente i sistemi dei clienti da eventuali attacchi. Un modello di notifica basato su sottoscrizione consente ai clienti di agire immediatamente per ridurre il rischio mentre vengono eseguiti patch e test del software. I clienti possono essere certi che i loro sistemi sono progettati e supportati ai massimi standard e possono gestire le proprie attività con fiducia, sapendo che Honeywell lavora per aiutarli a garantire la sicurezza dei loro sistemi.

Honeywell offre soluzioni per tutti e tre i principali sistemi operativi nell'area enterprise rugged mobile: Android, iOS e Windows. Per diversi anni, Honeywell ha mantenuto una posizione neutra rispetto alla scelta del sistema operativo sui computer portatili, incoraggiando i clienti a prendere in considerazione molti fattori per determinare quale fosse il miglior sistema operativo per il loro ambiente specifico.

Con la sua vasta quota di mercato e l'ampio ecosistema di app, sviluppatori e VAR, Android è diventato la scelta ovvia per molte imprese in svariati settori. La transizione ad Android implica la scrittura di nuove app, l'adattamento di alcuni flussi di lavoro e la modifica dell'utilizzo dei dispositivi mobili. Tutto questo può essere difficile da realizzare subito. Un modo per avere più tempo per prendere la giusta decisione è selezionare un hardware in grado di supportare più sistemi operativi. I computer portatili Honeywell delle serie CN75 e CK75, insieme al computer portatile Honeywell CN51, offrono la scelta di Windows Embedded Handheld o Android. Inoltre, i clienti che acquistano Windows Embedded Handheld possono convertire i propri dispositivi in Android in futuro. Ciò consente di continuare a eseguire le applicazioni precedenti esistenti fino a quando l'organizzazione non è pronta a passare ad Android.

Per ulteriori informazioni
www.honeywellaidc.com

Honeywell Safety and Productivity Solutions
Via Gerardo e Antonio Philips 12
20900 Monza
Italy
Tel.: +39 023 600 32 04
www.honeywell.com

Transizione del sistema operativo mobile – Approfondimenti e considerazioni | Rev A | 10/17

Honeywell