QUADRO DI SINTESI

Modernizzazione della sicurezza e della gestione di Windows 10 con VMware AirWatch, la soluzione per la gestione unificata degli endpoint

L'evoluzione richiede un'area di lavoro moderna

LA FORZA LAVORO odierna è più mobile e autonoma rispetto al passato. Con la proliferazione dei dispositivi mobili, i dipendenti utilizzano molteplici applicazioni, dispositivi e servizi basati su cloud. Scelgono sempre più spesso di gestire attività personali e di lavoro sullo stesso dispositivo e desiderano varietà di scelta, opzioni self-service e privacy. Se l'IT non riuscisse a soddisfare queste richieste, l'esperienza d'uso risulterebbe insoddisfacente, con dipendenti non coinvolti che ricorrerebbero con più frequenza all'IT ombra.

In più, l'organizzazione IT stessa si troverebbe a gestire dispositivi desktop e mobili in modo separato. L'IT ha affrontato la gestione dei dispositivi mobili servendosi di soluzioni di gestione dell'Enterprise Mobility (EMM, Enterprise Mobility Management). Tuttavia, i dispositivi desktop sono stati finora gestiti separatamente tramite strumenti di gestione del ciclo di vita dei PC (PCLM) tradizionali.

Ma questo è un modello frammentato non all'altezza delle aspettative di sicurezza e delle esigenze di budget dell'IT. Poiché gli utenti non sono più vincolati alla scrivania, e i tradizionali strumenti PCLM richiedono l'associazione dei dispositivi al dominio e alla rete aziendali per ricevere le policy IT nonché gli aggiornamenti delle patch per il sistema operativo, il rischio di non conformità e la proliferazione di vettori delle minacce aumentano.

Per rispondere alle esigenze della moderna forza lavoro occorre iniziare eliminando i sili di gestione e adottando un approccio alla gestione uniforme e incentrato sull'utente su tutti gli endpoint. Chris Silver, analista di Gartner, ritiene che "Il futuro della gestione degli endpoint risiede nel consolidare gli strumenti di gestione distinti tradizionalmente utilizzati per gestire i PC e i dispositivi mobili in un framework che abbracci entrambi".

L'introduzione di protocolli di gestione dei dispositivi mobili in Windows 10 dà all'IT l'opportunità di unire i team di gestione IT e di consolidare gli strumenti, ridurre i costi, migliorare l'efficienza dell'IT e potenziare la sicurezza aziendale. L'azienda può finalmente ottimizzare la gestione dei dispositivi degli utenti tramite l'implementazione di una soluzione per la gestione unificata degli endpoint (UEM) e gestire sia i desktop che i dispositivi mobili.

I LIMITI DELL'APPROCCIO TRADIZIONALE ALLA GESTIONE DEI PC

Il principale obiettivo delle organizzazioni IT dovrebbe essere creare esperienze d'uso soddisfacenti, che permettano agli utenti finali di lavorare in modo più efficace e produttivo. Eppure le esperienze d'uso per dispositivi mobili e PC sono per molti versi esattamente l'opposto. Sebbene il processo di distribuzione e configurazione di un dispositivo mobile sia diventato di tipo self-service ed efficiente, possono essere necessarie diverse settimane per distribuire un computer desktop o laptop e molte ore di lavoro per crearne l'immagine, configurarlo e gestirlo.

Gli utenti sono sempre più insoddisfatti per il fatto che la configurazione e la gestione dei dispositivi sono ottimizzate mentre la configurazione dei PC è un processo lento e restrittivo.

Dispositivo mobile

Un telefono viene pienamente configurato al momento dell'acquisto

Desktop e laptop

Occorrono diverse settimane di attesa per la configurazione dei dispositivi aziendali

Ma che cosa occorre cambiare?

1 Il sistema operativo

Il sistema operativo Windows è il primo elemento che occorre evolvere per poter gestire i requisiti della forza lavoro di oggi. Windows 10 è un sistema operativo incentrato sull'utente, con funzioni che offrono scelta, privacy e mobilità. L'aspetto senza dubbio più significativo è l'introduzione di un approccio completamente nuovo alla sicurezza e alla gestione del sistema operativo, che risulta più in linea con le moderne soluzioni EMM. L'insieme unificato di protocolli di gestione sui telefoni, tablet e PC con sistema operativo Windows 10 permette ora all'IT di consolidare gli strumenti di gestione, effettuare il provisioning pronto all'uso dei dispositivi e inviare policy e applicazioni over-the-air per assicurare l'operatività immediata degli utenti.

2 Gli strumenti di gestione

Gli strumenti di gestione dei PC esistenti non sono in grado di soddisfare i requisiti della forza lavoro odierna, che richiede di poter lavorare ovunque, in qualsiasi momento e con qualsiasi dispositivo. Gli utenti vogliono un'esperienza d'uso uniforme per accedere ai dati e alle applicazioni di lavoro su tutti i loro dispositivi. Soddisfare queste esigenze sta diventando sempre più difficile per i team IT che continuano a utilizzare strumenti tradizionali per gestire i PC in quanto sono:

- **Costosi**: gli approcci utilizzati finora per la gestione dei PC fanno un uso intenso di server e manodopera, richiedono l'adozione di più soluzioni software e si basano su metodi di gestione delle immagini e della configurazione complessi. Gestire i pacchetti software e le patch del sistema operativo è un processo noioso e l'IT ha la necessità di sviluppare e avere competenze interne per i silos di gestione di desktop e dispositivi mobili.
- **Non sicuri**: la gestione è per la gran parte affidata agli oggetti Criteri di gruppo (GPO), che sono possibili solo per i dispositivi associati a una rete e a un dominio. Con questo metodo, potrebbero occorrere diverse settimane o perfino diversi mesi prima che le policy di sicurezza, le patch del sistema operativo e gli upgrade delle applicazioni vengano completati, con conseguente possibile esposizione dell'azienda a maggiori rischi per la sicurezza. Ma ogni giorno vengono inventati nuovi vettori di attacchi, pertanto è sempre più difficile per l'IT avere la visibilità necessaria sullo stato e la conformità degli endpoint.
- **Limitanti**: gli approcci esistenti generano un senso di frustrazione negli utenti, che non hanno il pieno controllo sui loro dispositivi. Per potenziare la sicurezza, l'IT deve limitare i tipi di dispositivi e bloccare il sistema operativo solo con applicazioni e aggiornamenti affidabili. Questo sistema non lascia molto spazio per la personalizzazione e gli utenti hanno poche o nessuna funzionalità self-service. Questi vincoli generano un elevato numero di richieste per l'IT e un maggior numero di chiamate all'help desk, anche per attività semplici come l'installazione di un'applicazione in un dispositivo.

LA GESTIONE UNIFICATA DEGLI ENDPOINT È ORA UNA REALTÀ

L'introduzione delle API per la gestione dei dispositivi mobili in Windows 10 cambia radicalmente il modo in cui le aziende potranno gestire i loro PC. Tuttavia, diversamente dai sistemi iOS e Android, i PC pongono sfide specifiche, come:

- L'esigenza di supportare GPO e script complessi
- La creazione di pacchetti e la distribuzione delle applicazioni di Windows classiche (Win32)
- La verifica delle patch del sistema operativo prima che possano essere messe a disposizione degli utenti
- Le grandi dimensione di questi aggiornamenti e applicazioni causano vincoli di rete

Le aziende hanno bisogno di una piattaforma di gestione unificata degli endpoint che abbini le efficienze dell'IT e degli utenti finali offerte dalla EMM per i dispositivi mobili ai requisiti granulari della gestione dei PC tradizionale.

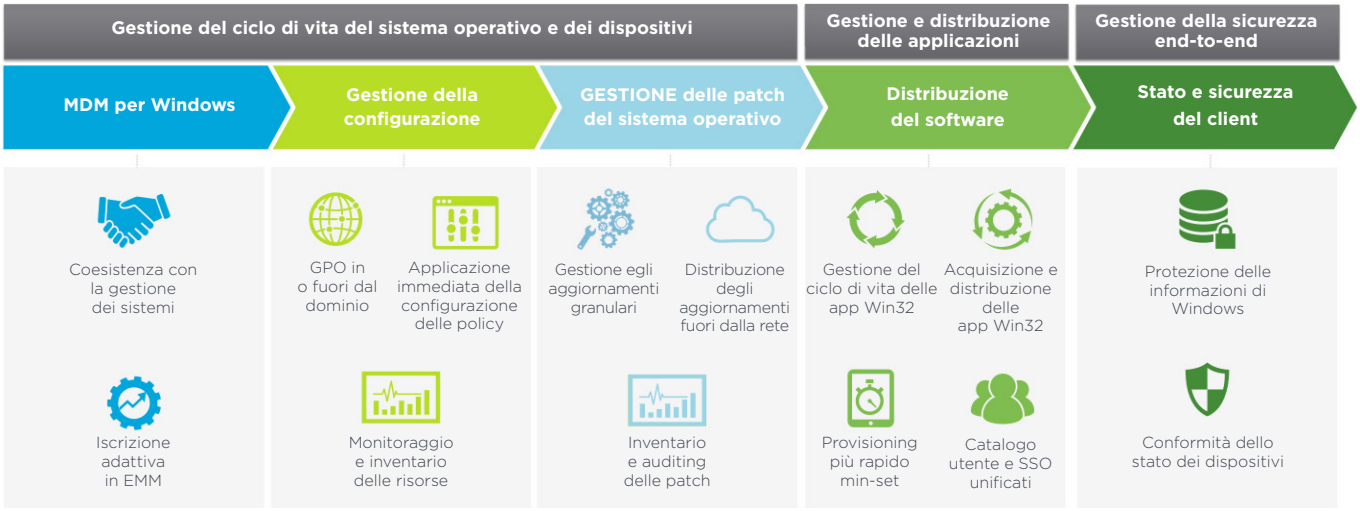
La gestione unificata degli endpoint con VMware AirWatch introduce un set completo di funzionalità di Windows 10 che consentono la distribuzione del sistema operativo, la configurazione, la distribuzione di applicazioni (incluse quelle Win32) e aggiornamenti e la sicurezza end-to-end. Adottando un approccio moderno cloud-first, si riducono i costi e il carico sull'IT ed è possibile raggiungere un'implementazione e una gestione più semplici e sicure di Windows 10. L'azienda può così:

- Passare da un processo di imaging costoso a un modello di distribuzione più semplice
- Supportare l'installazione di patch del sistema operativo e la distribuzione di software per dispositivi non legati al dominio o a una rete
- Effettuare il provisioning dell'accesso self-service degli utenti e dare loro la possibilità di scegliere tra le funzioni, i dispositivi e le applicazioni disponibili
- Stabilire la coesistenza di dati personali e di lavoro sui dispositivi
- Offrire visibilità, sicurezza e conformità immediate per tutti gli endpoint, dentro e fuori la rete

Con la soluzione UEM AirWatch, la gestione di Windows si applica a tutti i casi d'uso, come:

- Distribuzione di Windows 10 ai lavoratori remoti
- Integrazione dei dispositivi BYOD dei dipendenti
- Implementazione di distribuzioni aziendali tra diverse filiali
- Gestione di uno speciale terminale linea di business

AirWatch UEM offre una gestione dei dispositivi più semplice, più sicura e più conveniente



DISTRIBUZIONE DI SICUREZZA E GESTIONE DI WINDOWS CON APPROCCIO CLOUD-FIRST

MDM per Windows

AirWatch supporta flussi di lavoro coerenti per l'iscrizione dei dispositivi adatta a diversi casi d'uso, come i dispositivi BYOD o di proprietà dell'azienda, che si tratti di dispositivi nuovi, esistenti o associati a un dominio. Con AirWatch, un generico dispositivo OEM può essere pienamente trasformato in un dispositivo affidabile e pronto all'uso senza necessità di crearne l'immagine, con conseguenti risparmi di tempo e denaro dell'IT. Oltre ai flussi di lavoro abilitati dall'IT, AirWatch è inoltre in grado di supportare gli utenti finali con l'integrazione intuitiva e self-service dei dispositivi.

Per quanto riguarda gli utenti o i collaboratori BYOD, AirWatch consente perfino un'iscrizione granulare nella gestione sulla base dei requisiti di sicurezza e sensibilità delle applicazioni. Ad esempio, l'accesso alle applicazioni per la produttività di base può essere concesso tramite un catalogo personalizzato delle applicazioni aziendali basato sull'identità e i diritti dell'utente. Tuttavia, l'accesso alle applicazioni che contengono dati aziendali sensibili può essere concesso solo se il dispositivo viene pienamente gestito con AirWatch.

AirWatch è in grado di gestire i dispositivi Windows integrati tramite l'utilizzo di questo moderno framework mobile-cloud e di configurare le policy istantaneamente e over-the-air. Con ogni upgrade di Windows 10, Microsoft mira a espandere l'insieme comune di protocolli di gestione disponibili ai fornitori di soluzioni EMM. Tutto questo sta rendendo l'attività di gestione più simile alle impostazioni e ai profili utente utilizzati per i dispositivi mobili. Ad esempio, l'applicazione di codici, la configurazione dell'e-mail, l'attivazione dell'accesso alle reti Wi-Fi e VPN aziendali e l'applicazione di limitazioni all'uso di dispositivi e applicazioni sono tutte operazioni il cui obiettivo è semplificare la configurazione del sistema operativo e potenziare la sicurezza.

Gestione della configurazione

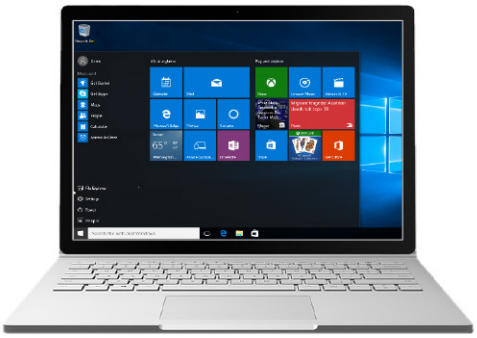
Quando si gestiscono PC Windows, l'IT avrà spesso requisiti di automazione complessi che richiedono l'applicazione di script altrettanto complessi, policy GPO e altre impostazioni di gestione dei PC tradizionali. Ad esempio, un'azienda può richiedere che i propri desktop abbiano un wallpaper personalizzato, che vengano rimossi i bloatware e vengano definite policy antivirus e per il firewall. Le funzionalità di gestione della configurazione offerte da AirWatch consentono all'IT di creare soluzioni che includono questi file, applicazioni o impostazioni personalizzate. Queste soluzioni possono quindi essere distribuite ai dispositivi in modo immediato su qualsiasi rete e anche essere associate a una più complessa sequenza di attività e condizioni di installazione.

Gestione delle patch del sistema operativo

Con Windows Update "as-a-Service", Microsoft sta lavorando per offrire aggiornamenti cumulativi del sistema operativo over-the-air. Gli aggiornamenti che sono stati ampiamente testati vengono spediti come Servicing Branch specifico per l'azienda. Anche se la distribuzione nel cloud e questo modello di servizi offrono indiscutibilmente dei vantaggi, l'IT ha ancora paura di perdere il controllo su:

- Quali aggiornamenti vengono distribuiti
- Rischio di danneggiare il sistema operativo per mancanza di rigorose verifiche interne degli aggiornamenti
- Vincoli di rete, poiché gli aggiornamenti hanno ora dimensioni di diversi gigabyte

Wi-Fi | VPN | Cert. | E-mail | Codici | Conformità e limitazioni | Crittografia | Firewall e antivirus | GESTIONE delle licenze del SO



AirWatch semplifica la configurazione e la gestione dei dispositivi over-the-air.

Con AirWatch, l'IT può distribuire e/o rimandare gli aggiornamenti e le patch del sistema operativo sulla base della priorità dei dispositivi e delle finestre di manutenzione desiderate. Consente all'IT di auto-approvare o non consentire gruppi di aggiornamenti specifici, ad esempio per applicazione, sviluppatore, sicurezza e così via, in base alla sensibilità degli utenti e agli aggiornamenti di funzioni e sicurezza. Avvalendosi del caching peer-to-peer, AirWatch consente l'ottimizzazione della distribuzione degli aggiornamenti ed evita la congestione della rete. L'IT può ricevere l'inventario dettagliato ed eseguire l'auditing di conformità dei singoli aggiornamenti di Windows e può superare le sfide associate all'installazione di patch al di fuori della rete.

Distribuzione del software

Con la Universal Windows Platform (UWP), Microsoft ha unificato l'esperienza d'uso delle applicazioni su tutti i dispositivi che eseguono Windows 10. Le applicazioni UWP pubbliche possono ora essere distribuite tramite il Windows Store in modo analogo a quanto avviene con altri store sui sistemi operativi per dispositivi mobili, oppure tramite un business store interno personalizzato per l'azienda. AirWatch si integra con il Windows Store e il Windows Store for Business per ottimizzare la distribuzione di queste applicazioni moderne.

Tuttavia, la maggior parte del software per le aziende di Windows continua a essere costituito dalle classiche applicazioni Win32, che hanno grandi dimensioni e possono essere complesse da impacchettare, distribuire e gestire. Ciò rende la distribuzione del software una delle più grandi sfide della gestione di Windows con soluzioni EMM. AirWatch risolve questa situazione colmando le lacune nella gestione del ciclo di vita delle applicazioni UWP e Win32.

Con AirWatch, l'IT è in grado di consolidare la Mobile Application Management e la distribuzione del software Win32 tradizionale in un'unica console di amministrazione. Gli amministratori possono gestire le patch delle applicazioni di terze parti, applicare dipendenze e perfino definire condizioni o contingenze per l'installazione delle applicazioni.

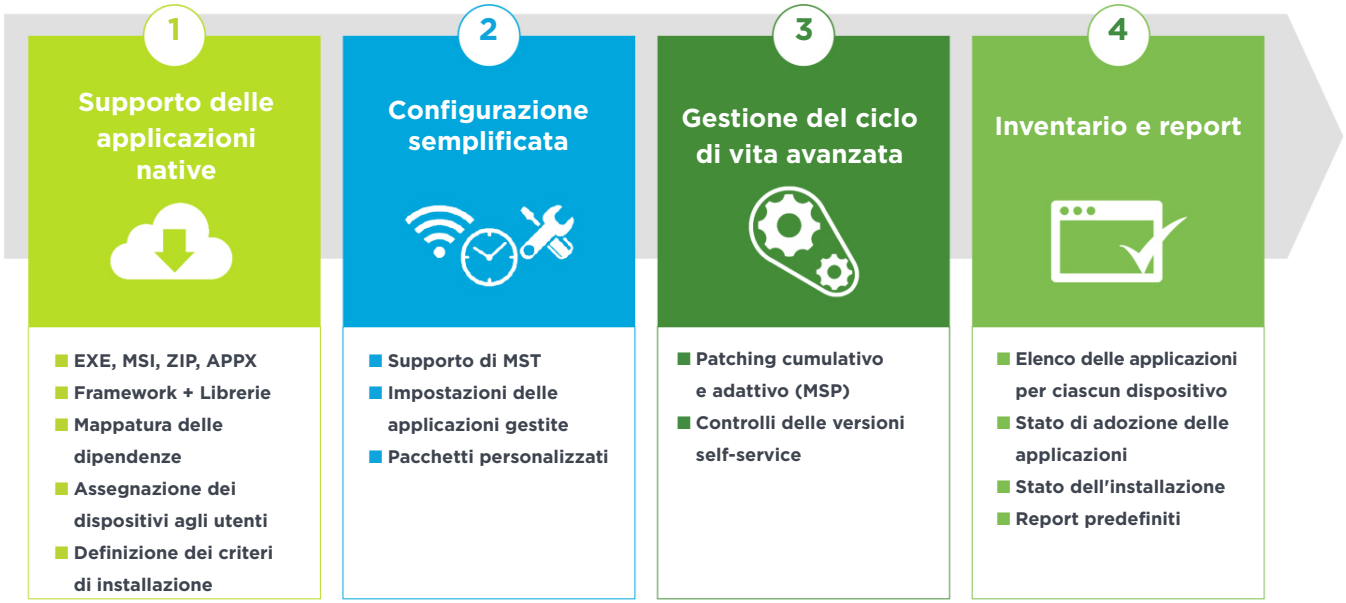
Con App Stacks, AirWatch introduce un nuovo approccio alla distribuzione del software che supera i problemi di pacchettizzazione delle applicazioni e di installazioni inaffidabili. L'IT può anche distribuire le applicazioni Win32 più velocemente su qualsiasi dispositivo Windows con la stessa affidabilità e la stessa semplicità della distribuzione di una mobile app. Dal punto di vista dell'utente finale, AirWatch offre un catalogo self-service e un'esperienza Single Sign-on (SSO) uniforme su tutte le applicazioni di Windows, native, SaaS e remote.

Stato e sicurezza dei client

Le problematiche odierne legate alla sicurezza informatica richiedono anche sicurezza end-to-end. AirWatch consente di ottenere la fiducia degli utenti, rafforza le difese del sistema operativo contro nuove minacce e offre la separazione dei dati di lavoro da quelli personali per proteggere i dati aziendali inattivi, in uso e in transito.

- **Fiducia degli utenti**: anche le password più sicure sono vulnerabili e possono essere rubate in vari modi, ad esempio con attacchi di phishing, la registrazione delle pressioni sui tasti e l'introduzione di malware. AirWatch si integra con le funzioni di gestione dell'identità di Windows 10 per impostare policy per l'autenticazione senza password

Funzionalità di gestione delle applicazioni Win32



che si servono di gesti o di un PIN. Le aziende possono attivare l'autenticazione multifattore (MFA) pronta all'uso e proteggersi così dagli attacchi di tipo Pass-the-Hash.

■ **Rafforzamento del sistema operativo**: con AirWatch, l'IT adotta attivamente misure di sicurezza per evitare il download o l'esecuzione di applicazioni inaffidabili o non approvate. AirWatch verifica l'integrità e la conformità dei dispositivi in tempo reale, bloccando automaticamente l'accesso alle applicazioni e ai servizi aziendali per i dispositivi non conformi.

■ **Protezione dei dati**: prevenire la perdita dei dati è al momento la priorità numero uno, in quanto la proliferazione dei dispositivi mobili accresce la possibilità di smarrimento o furto dei dati. Inoltre, è sempre più frequente per gli utenti svolgere attività di lavoro e personali sugli stessi apparecchi. AirWatch consente di impostare policy per la crittografia dei dati, permette ad amministratori e utenti finali di cancellare i dati in remoto se un dispositivo viene smarrito o rubato, e assicura la separazione tra dati di lavoro e dati personali tramite l'adozione di funzioni di containerizzazione del sistema operativo Windows.

AirWatch UEM aiuta l'azienda ad adottare la gestione della sicurezza end-to-end in maniera efficiente ed economica.

SICUREZZA PER TUTTI GLI ENDPOINT CON UN'UNICA PIATTAFORMA

La soluzione UEM deve essere per sua concezione indipendente dalla piattaforma e in grado di offrire un'unica soluzione per gestire qualsiasi dispositivo e qualsiasi sistema operativo con qualsiasi caso d'uso. In tal modo viene garantita un'esperienza d'uso coerente agli utenti finali, indipendentemente dal dispositivo utilizzato per accedere all'ambiente aziendale.

AirWatch UEM consente di adottare un approccio olistico e incentrato sull'utente per la gestione e la protezione di qualsiasi endpoint da un'unica piattaforma. Supporta la distribuzione globale tra più divisioni, regioni e reparti in una console unica con un'architettura multi-tenant. AirWatch UEM si integra con i sistemi aziendali per sfruttare appieno gli investimenti effettuati nell'infrastruttura esistente ed estendere tali servizi a tutti gli endpoint.

Con VMware AirWatch UEM, l'IT può automatizzare i processi tramite motori di policy dinamici e intelligenti alle piattaforme Windows 10. Ciò riduce le attività manuali che ricadono sull'IT e offre funzionalità self-service, con conseguente riduzione dei costi di assistenza.

Sei pronto a ripensare la gestione degli endpoint? Ti invitiamo a registrare fino a 100 dispositivi in una prova gratuita valida per 30 giorni. Per ulteriori informazioni, visita il sito web.