WHITE PAPER - FEBBRAIO 2017

CINQUE FASI CRUCIALI PER MODERNIZZARE L'AMBIENTE WINDOWS

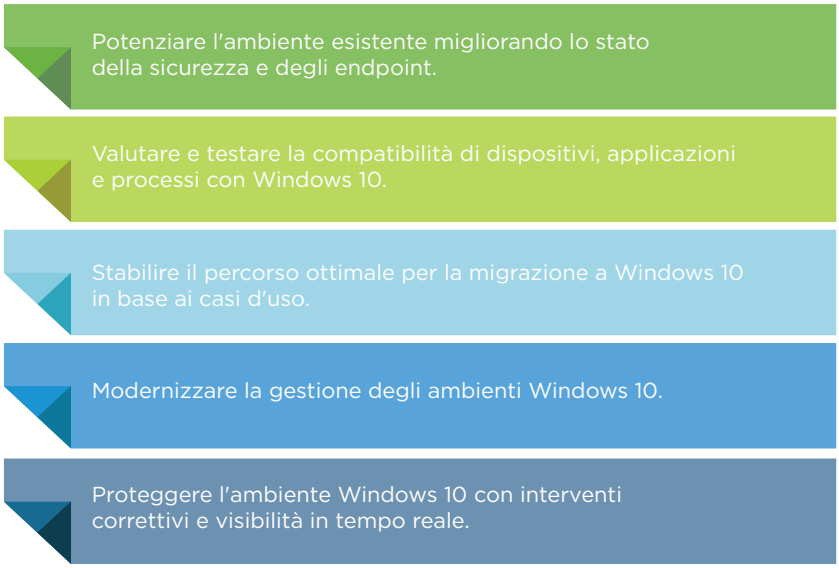
Guida per la valorizzazione ottimale degli investimenti in risorse Windows e l'illustrazione del percorso verso Windows 10 per le distribuzioni virtuali e fisiche.

vmware®

Windows fa girare il mondo

Windows viene utilizzato su oltre 1,5 miliardi di dispositivi*. Negli ultimi 30 anni la maggior parte delle organizzazioni di tutto il mondo ha scelto Windows come standard realizzando investimenti significativi negli ambienti Microsoft in uso (licenze, configurazione, servizi professionali e infrastruttura per Active Directory, Microsoft Exchange, gestione del ciclo di vita del PC e così via). Microsoft continua inoltre a sviluppare soluzioni che aiutano le organizzazioni a completare il passaggio al cloud con prodotti come Microsoft Office 365 e Azure Active Directory e con la creazione di un innovativo framework di gestione del mobile-cloud in Windows 10.

Allo stesso tempo, i reparti IT si trovano costantemente sotto pressione per ridurre i costi rafforzando al contempo la sicurezza e aumentando la produttività dei dipendenti con le tecnologie più all'avanguardia. Windows 10 offre un'esperienza più soddisfacente per gli utenti e opportunità per i team IT di adottare un approccio sostanzialmente diverso alla gestione e alla sicurezza al fine di ridurre il proprio carico di lavoro. Tuttavia, per ottimizzare e valorizzare al meglio l'ambiente Windows in uso le organizzazioni devono intraprendere un determinato percorso:



In questo white paper verranno illustrate le cinque fasi che le organizzazioni possono seguire per ottimizzare gli investimenti esistenti nelle risorse Windows e scoprire come adottare un approccio moderno alla gestione e alla sicurezza nell'ambito della transizione a Windows 10.

Fase 1: messa a punto dell'ambiente Windows per aumentarne durata ed efficienza

Gli automobilisti più responsabili eseguono periodicamente la messa a punto della loro vettura ispezionando, riparando o sostituendo le candele d'accensione, i filtri dell'aria e altri componenti che non funzionano al meglio delle prestazioni. A volte fanno ricorso a soluzioni complementari, come usare un olio per motori ad alto chilometraggio o un additivo per rimuovere i depositi di carbonio dalle tubazioni del carburante. Risultato: i consumi si riducono e la durata di vita della vettura aumenta.

Quando avete eseguito l'ultima messa a punto del vostro ambiente Windows? La prima fase per un ambiente Windows all'avanguardia consiste nel potenziare i processi, le tecnologie e le funzioni di reportistica esistenti per rendere più produttiva l'azienda e più soddisfatti gli utenti finali. Sapete su quante macchine della vostra flotta è stata correttamente implementata la patch che avete inviato lo scorso martedì? Sapete quanti utenti stanno eseguendo un'app che ha mancato un aggiornamento critico per la vulnerabilità? Avete preso in considerazione le innovazioni offerte da smartphone e tablet potenzialmente in grado di semplificarvi la vita con i PC?

- Quando avete eseguito l'ultima messa a punto del vostro ambiente Windows?
- Sapete su quante macchine della vostra flotta è stata correttamente implementata la patch che avete inviato lo scorso martedì?
- Sapete quanti utenti stanno eseguendo un'app che ha mancato un aggiornamento critico per la vulnerabilità?
- Avete preso in considerazione le innovazioni offerte da smartphone e tablet potenzialmente in grado di semplificarvi la vita con i PC?

I feedback che riceviamo dai clienti sono tutti sulla stessa linea. Gli utenti desiderano essere produttivi ovunque si trovino e su qualsiasi dispositivo scelgano di usare. Spesso si trovano ad accedere alle risorse aziendali fuori rete da diversi tipi di dispositivi, aumentando così il numero dei vettori di minaccia per l'organizzazione. Il team IT deve avere una visibilità in tempo reale sull'ambiente Windows in uso per poter sapere quali dispositivi non sono aggiornati con le ultime patch e quali eseguono app non firmate o versioni meno recenti delle dipendenze app (ad es. Java, .NET) esponendo il dispositivo e la rete aziendale a potenziali attacchi. Inoltre il team deve poter agire sulla base di tali informazioni, ad esempio distribuendo una patch, terminando un processo fuori controllo o eseguendo in remoto la cancellazione di un dispositivo che rappresenta una minaccia per la sicurezza.

Sicurezza e visibilità in tempo reale dell'ambiente in uso

Immaginiamo di poter ottenere una visibilità completa su tutti gli endpoint in 15 secondi al massimo o di poter interrogare un intero ambiente digitando una semplice domanda, come per le ricerche di Google, ottenendo in pochi secondi risultati provenienti anche da milioni di endpoint e raccogliendo in un istante informazioni critiche su cui basare gli interventi. Ora tutto questo è possibile. VMware® funziona con le versioni desktop e server di Windows 7, 8.1 e 10 sia virtuali che fisiche e consente di:

- Individuare gli endpoint non gestiti e assumerne il controllo
- Rilevare le minacce avanzate su milioni di endpoint in pochi secondi
- Correggere rapidamente gli endpoint compromessi secondo necessità
- Ripristinare gli endpoint Windows compromessi con un'immagine gold

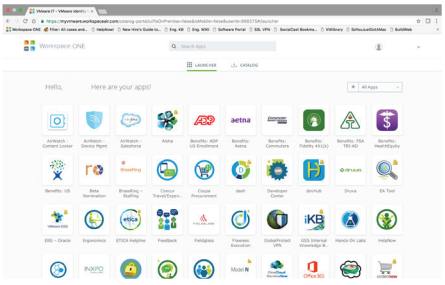
La piattaforma "attraversa" l'intera organizzazione per proteggere gli endpoint, per dare alle operation IT una visibilità in tempo reale sull'inventario software e sull'utilizzo dettagliato delle risorse, nonché per distribuire patch e applicazioni secondo necessità. Per i clienti che pianificano il passaggio a Windows 10, VMware consente di esaminare l'ambiente esistente per risolvere eventuali problemi e semplificare la transizione a Windows 10.

VMware offre inoltre un metodo all'avanguardia per proteggere e gestire i dispositivi mobili, gli endpoint Windows e i server. Grazie alle integrazioni con l'ecosistema VMware, è possibile ottenere una maggiore conformità, un contenimento più rapido delle minacce, oltre a interventi correttivi personalizzabili e adattabili ai diversi livelli di minacce, attraverso policy dinamiche di configurazione e gestione.

Ad esempio, è possibile utilizzare VMware per eseguire interrogazioni e rilevare gli endpoint non conformi, mettendo quindi in quarantena i dispositivi interessati. Una volta completato il contenimento della minaccia, VMware può comunicare agli utenti finali le violazioni della conformità per consentire agli amministratori IT di distribuire la soluzione necessaria e quindi ripristinare lo stato di conformità degli endpoint.

Configurazione over-the-air e catalogo consolidato delle app

Ricordate quando è stata l'ultima volta che un dirigente vi ha chiamati mentre era in viaggio per comunicarvi di aver smarrito il suo laptop? In un caso come quello, se non si applica la crittografia BitLocker, le informazioni aziendali sensibili possono finire nelle mani di utenti non autorizzati, senza possibilità di recuperarle. Distribuendo invece una soluzione di gestione unificata degli endpoint (UEM), è possibile eseguire una cancellazione in remoto per impedire la perdita dei dati.



Le soluzioni EMM offrono da sempre alle organizzazioni la possibilità di configurare il Wi-Fi, di eseguire il setup di una rete VPN, di accedere a un app store aziendale consolidato e di eseguire una cancellazione in remoto su iOS, Android e altri sistemi operativi mobili. Distribuendo soluzioni EMM compatibili con i tradizionali ambienti Windows, le organizzazioni possono potenziare gli strumenti di gestione del ciclo di vita dei PC estendendo le stesse funzionalità dai sistemi operativi mobili per offrire una migliore esperienza d'uso, aumentare la sicurezza e far risparmiare tempo ai team IT.

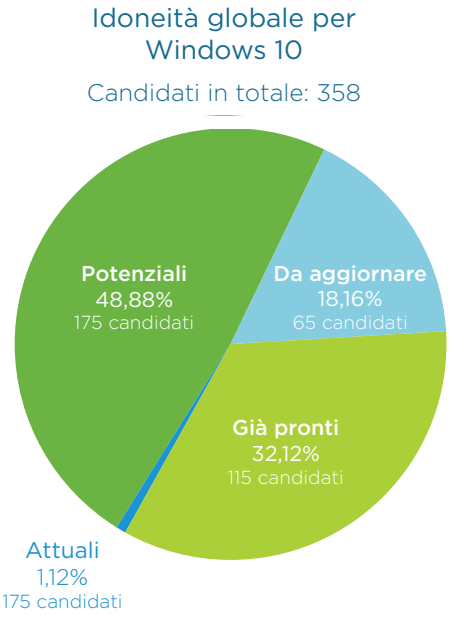
Supporto per i lavoratori remoti e distribuzione delle applicazioni con la virtualizzazione

Quando è stata l'ultima volta che avete valutato i casi d'uso e le esigenze dei vostri utenti finali? Potreste avere dei desktop virtuali per gli scenari comuni, come call center e sviluppatori remoti, ma avete pensato ad altri modi per estendere le risorse ai vostri dipendenti, collaboratori e partner? Con la virtualizzazione dei desktop e delle applicazioni, sarete in grado di fornire le risorse necessarie per gli utenti sui loro dispositivi personali o su qualsiasi altro dispositivo. Alcune applicazioni possono richiedere una specifica versione di sistema operativo, browser o plug-in. Per poterle eseguire ovunque, indipendentemente dal sistema operativo degli utenti, è necessario virtualizzarle.

Grazie a VMware, è possibile distribuire centralmente i desktop virtuali secondo necessità, adottare la strategia BYOD, eliminare il downtime dovuto a endpoint persi o danneggiati, migliorare la sicurezza conservando i dati al sicuro nel data center e incrementare i profitti evitando gli aggiornamenti hardware o riducendo i costi degli endpoint. Ne deriva una strategia di End-user computing più semplice, sicura e scalabile.

Alla scoperta di un nuovo mondo con il passaggio a Windows 10

Si dice che se Henry Ford avesse ascoltato i suoi clienti, avrebbe dato loro dei cavalli più veloci. L'automobile costruita da Ford ha cambiato il mondo dei trasporti risolvendo il problema in un modo completamente diverso. In modo analogo, Windows 10 si differenzia completamente dai suoi predecessori ridefinendo il modo in cui l'IT gestisce l'intero ciclo di vita di PC, smartphone, tablet e qualsiasi altro endpoint dotato dell'ultimo sistema operativo offerto da Microsoft.



Fino alla release di Windows 10, l'approccio dei reparti IT all'ambiente in uso somigliava molto a quello di un cliente alla ricerca di prodotti in un centro commerciale: mettere insieme tecnologie eterogenee che non funzionavano bene insieme per risolvere diversi problemi relativi a configurazione, distribuzione del software, installazione di patch, malware e sicurezza.

Con Windows 10, Microsoft ha introdotto una nuova possibilità che funziona invece come l'e-commerce: è comodo, usa tecnologie che funzionano bene insieme e apre la strada a nuove opportunità prima inesistenti. Dopo aver parlato con centinaia di clienti che sono già passati a Windows 10 o che ne stanno mettendo a punto l'implementazione, abbiamo scoperto che, una volta migliorata la sicurezza negli ambienti esistenti, restano altre quattro fasi chiave per assicurare il buon esito della distribuzione di Windows 10:

Valutazione ▶ Migrazione ▶ Gestione ▶ Sicurezza

Fase 2: valutazione dell'ambiente esistente per risolvere tutti i dubbi relativi alle distribuzioni fisiche e virtuali

Per molte organizzazioni è difficile capire da dove iniziare per eseguire la migrazione a Windows 10: individuare le macchine esistenti che sono compatibili con Windows 10, i casi d'uso più adatti per la virtualizzazione del desktop e così via. Con il giusto strumento di valutazione dei desktop, le organizzazioni possono ricevere preziose indicazioni su quali macchine e casi d'uso sono più adatti a una migrazione fisica in-place a Windows 10 e quali invece sono più idonei all'esecuzione di un desktop virtuale on-site o dal cloud, ottenendo in tal modo una comprensione di base dell'ambiente esistente per stabilire l'approccio migliore alla migrazione a Windows 10. Per ulteriori informazioni sullo strumento di valutazione, visitare la pagina assessment.vmware.com.

Come per i precedenti upgrade a nuove versioni di Windows, gli amministratori IT responsabili degli ambienti desktop fisici o virtuali devono testare le applicazioni per individuare eventuali problemi di compatibilità prima di eseguire la migrazione della flotta a Windows 10. Se le applicazioni non funzionano con Windows 10, i team IT possono distribuirle come app virtuali in modo che possano continuare a funzionare dopo la migrazione a Windows 10, consentendo agli utenti di svolgere comunque il proprio lavoro. Questa situazione si verifica, ad esempio, con le applicazioni legacy come Internet Explorer 6.

Fase 3: sviluppo del piano per la migrazione delle macchine virtuali e fisiche

Secondo Microsoft, il 96% delle aziende sta eseguendo un programma pilota su Windows 10. Tuttavia, molte sono ancora nella fase di messa a punto dei piani per la migrazione. Le domande che possiamo porre ai clienti per ottenere una base di confronto da usare come guida nel percorso verso Windows 10 sono molte.

- State pianificando di adottare Windows 10 nell'arco dei prossimi 3-4 anni, man mano che i PC vengono aggiornati?
- State pianificando una migrazione in-place o con immagini personalizzate di tutte le macchine esistenti?
- State pianificando di virtualizzare gli endpoint che non sono in grado di supportare Windows 10?
- Volete dedicarvi ai casi d'uso aziendali in cui applicazioni e desktop virtuali possono migliorare l'efficienza?
- Il vostro programma prevede una combinazione delle precedenti opzioni?

Ogni organizzazione deve determinare il percorso di migrazione più adatto alle proprie esigenze. Ecco alcuni dei modi più comuni in cui aiutiamo le organizzazioni ad affrontare tale percorso:

Aggiornamento

Mentre i dispositivi vengono aggiornati nell'arco di 3-4 anni, le organizzazioni completano il passaggio a Windows 10 e gestiscono tutti i nuovi dispositivi con il moderno framework di gestione unificata degli endpoint (UEM) che consente di semplificare le attività IT, ridurre i costi di gestione e offrire l'esperienza migliore possibile agli utenti finali.

Migrazione

- In-place: le organizzazioni sfruttano gli strumenti di migrazione in-place per il passaggio delle macchine dalle versioni precedenti del sistema operativo all'immagine di base di Windows 10, effettuando il provisioning delle app e delle policy consigliate dall'azienda grazie alla soluzione UEM.
- Immagine personalizzata: anziché passare all'immagine di base del sistema operativo, le organizzazioni possono eseguire la migrazione a un'immagine consigliata dall'azienda con app e dati personalizzati, registrandosi automaticamente nella soluzione di gestione con UEM.

Virtualizzazione

- Le app e i desktop virtuali vengono aggiornati centralmente e distribuiti agli utenti finali sui dispositivi esistenti, garantendo in tal modo il supporto di vari casi d'uso, come ad esempio:
  - Le macchine esistenti che non supportano Windows 10 ricevono un desktop virtuale
  - Le organizzazioni prendono in considerazione i desktop virtuali per gli scenari con laptop BYO
  - Le applicazioni mission critical che non sono compatibili con Windows 10 possono essere virtualizzate
  - Le organizzazioni adottano l'isolamento di Internet o dei dati per le distribuzioni con requisiti di sicurezza elevati

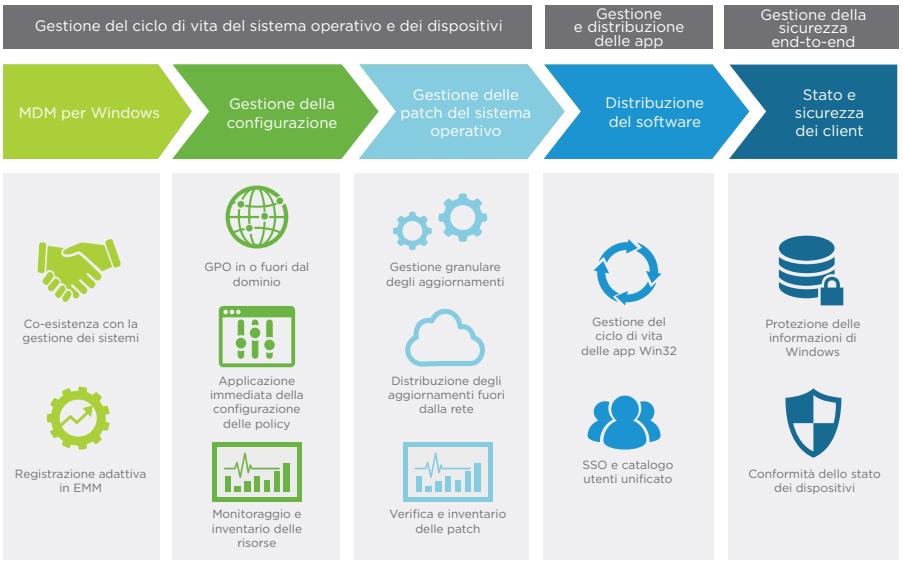
Fase 4: valutazione di soluzioni UEM per le macchine virtuali nel nuovo framework Windows

I tradizionali processi per l'imaging, la configurazione e il setup completo di un PC fisico possono richiedere diverse ore. Nel tempo, i residui dei file di registro e delle applicazioni riducono le prestazioni del sistema (con conseguente scostamento delle immagini), causano problemi di prestazioni per gli utenti finali e spesso richiedono l'intervento del team IT per il re-imaging dei dispositivi (con conseguenti disagi per gli utenti e perdita di tempo prezioso).

Per gestire l'ambiente Windows in uso, la maggior parte delle organizzazioni usa strumenti di gestione del ciclo di vita dei PC con centinaia di GPO, script personalizzati e altri strumenti eterogenei. Sfortunatamente gli strumenti PCLM legacy hanno diversi limiti, come ad esempio l'impossibilità di eseguire azioni sui dispositivi fuori dal dominio e dalla rete aziendale, un'infrastruttura costosa da gestire, processi molto impegnativi (come l'imaging) e così via.

Il vantaggio dei moderni smartphone consiste nella possibilità di entrare in un negozio, acquistare un dispositivo, inserire le proprie credenziali e ottenere automaticamente l'accesso a tutti i servizi e le applicazioni over-the-air in pochi minuti. Perché gli utenti dei PC non dovrebbero poter fare lo stesso? Ebbene, con Windows 10 in effetti possono. Windows 10 gestito con soluzioni UEM offre alle organizzazioni un nuovo modo per supportare la flotta di desktop e garantire un'esperienza simile a quella degli utenti di smartphone e tablet. Semplicemente inserendo il proprio indirizzo e-mail aziendale e la relativa password, i dispositivi vengono configurati over-the-air in pochi minuti con tutti i servizi, le applicazioni e le policy aziendali necessari per lavorare. Il nuovo approccio ridefinisce il modo in cui l'IT gestisce l'intero ciclo di vita di PC, smartphone, tablet e ogni altro tipo di endpoint in modo coerente da una console unificata.

Sicurezza e gestione di Windows con un moderno approccio cloud-first



Niente più ore e ore passate a eseguire l'imaging di ogni singola macchina. Niente più patch del martedì. Niente più azioni non eseguibili sugli utenti che non si trovano nella sede aziendale. Grazie alla distribuzione di soluzioni UEM nelle macchine con Windows 10, i team IT hanno più tempo da dedicare alla gestione delle attività di business e un'ambiente molto più sicuro. Da parte loro, gli utenti ottengono un catalogo di applicazioni unificato sul PC con Windows 10, sul tablet e sullo smartphone che usano, oltre a un portale self-service in cui possono trovare da soli le soluzioni ai problemi più comuni anziché monopolizzare il tempo dei team IT.

Fase 5: rafforzamento della sicurezza con visibilità in tempo reale sull'ambiente

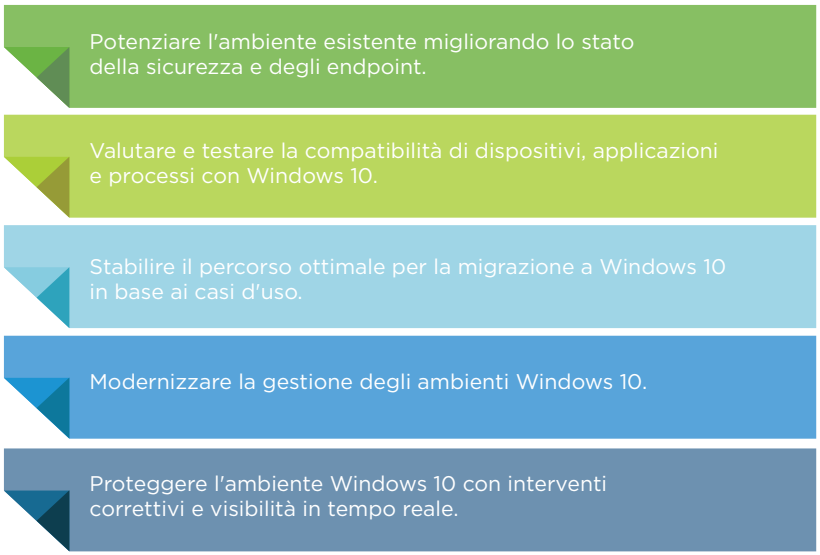
Andrew Grove, cofondatore ed ex CEO di Intel Corporation, aveva un motto: "Solo i paranoici sopravvivono". Questo stesso principio, che sta alla base del successo di Intel, deve essere anche il mantra dell'intero settore IT. In passato le organizzazioni disponevano di un ambiente operativo standard: un tipo di dispositivo aveva un sistema operativo con un set di applicazioni pre-approvate su una specifica rete. Ora, invece, l'IT deve supportare diversi tipi di sistemi operativi in esecuzione su dispositivi di qualsiasi tipo con combinazioni uniche di applicazioni eseguite nella rete aziendale o al di fuori di essa.

Dovendo supportare un ambiente operativo così dinamico e contrastare una gamma sempre più ampia di attacchi informatici alla sicurezza, i team IT sono stati costretti ad adottare un modello Zero Trust per proteggere i dati aziendali. Con VMware, i team IT possono rafforzare il sistema operativo consentendo autenticazioni senza password, impedendo l'esecuzione di app non approvate e non firmate, eseguendo il monitoraggio per individuare eventuali dispositivi compromessi ed eseguendo interventi correttivi automatizzati senza la necessità di richieste di assistenza IT. Tali azioni possono includere l'immediata restrizione dell'accesso alle risorse aziendali nel momento in cui un sistema operativo viene identificato come compromesso o perfino l'esecuzione di un comando di cancellazione in remoto per i dispositivi smarriti o rubati. VMware offre anche le funzionalità indicate in precedenza per la sicurezza e la visibilità in tempo reale dei dispositivi con Windows 10.

Per ulteriori informazioni su come VMware può aiutare le organizzazioni a modernizzare l'ambiente Windows in uso e ottenere il massimo dagli investimenti in risorse Microsoft, visitare il sito web www.WindowsUEM.com/it

Ottimizzazione del valore dell'ambiente in uso

Abbiamo visto solo una minima parte di ciò che è possibile fare grazie a VMware per ottimizzare il valore degli investimenti nelle risorse Microsoft. Ecco un rapido riepilogo dei cinque principali modi in cui VMware può sostenere le iniziative delle organizzazioni per arricchire l'ambiente esistente con funzionalità aggiuntive e completare la migrazione a Windows 10:



Oltre a cercare soluzioni a supporto delle distribuzioni di Windows, è possibile che le organizzazioni investano in risorse Microsoft in altri modi, come ad esempio passando a Office 365, ad Azure Active Directory e così via. Le soluzioni di End-user computing offerte da VMware possono aiutarle a distribuire e configurare in modo più semplice i servizi e le app di Office, oltre che a collegare le policy e le credenziali di Directory per le identità federate e il Single Sign-on delle applicazioni.

1,5 miliardi di dispositivi: http://www.computerworld.com/article/2919104/windows-pcs/where-will-microsoft-find-1-billion-devices-for-windows-10.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Inc. - Via Spadolini, 5 - Edificio A - 20141 Milano - Tel.: (+39) 02 3041 2700 Fax: (+39) 02 3041 2701 www.vmware.it