

# Tre segnali che indicano di passare a un workspace digitale

Andate oltre il desktop per migliorare la produttività degli utenti, favorire il reparto IT e mantenere i dati al sicuro

---

Non molto tempo fa, un desktop aziendale o virtuale era tutto ciò che serviva per un rapido onboarding dei dipendenti. Ma per affrontare il futuro, non è più sufficiente. Se desiderate rimanere al passo con i crescenti requisiti di produttività dell'organizzazione, sono tre le tendenze emergenti che indicano che è il momento di passare al workspace digitale sicuro.

- 1. Crescita della forza lavoro mobile**
- 2. Modernizzazione delle applicazioni**
- 3. Scomparsa del perimetro di sicurezza**

---

Scoprite come pensare oltre il desktop può aiutarvi a migliorare la produttività degli utenti, consentire all'organizzazione IT di essere più agile e proteggere meglio i dati dell'azienda.



Lo sapevate?



Oltre 1/3

dei dipendenti cambierebbe lavoro per avere maggiore flessibilità<sup>1</sup>.



Solo il 57%

delle persone lavora fisicamente al fianco dei propri colleghi il 100% del tempo<sup>1</sup>.

### 1. Una forza lavoro mobile in crescita

I dipendenti vogliono scegliere dove e come lavorare. Infatti, il report di una ricerca condotta da Gallup suggerisce che il 37% dei dipendenti cambierebbe lavoro per avere maggiore flessibilità, almeno parte del tempo. La ricerca rivela inoltre che solo il 57% dei dipendenti condivide un luogo di lavoro con i colleghi il 100% del tempo<sup>1</sup>. Per aumentare la produttività, l'agilità e l'esperienza dei dipendenti, le aziende ora riconoscono le potenzialità offerte dal lavoro in remoto, sia esso svolto da casa, presso la sede di un cliente, in un hotel o in un bar. Tocca al reparto IT il compito di evolversi di conseguenza. Anche se è possibile fornire applicazioni virtuali a una forza lavoro mobile, ci sono altri fattori che rendono la virtualizzazione più problematica, in particolare le applicazioni moderne.

### 2. Modernizzazione delle applicazioni

Sempre più spesso, le applicazioni vengono progettate per funzionare su qualsiasi piattaforma. Microsoft Office è un buon esempio di applicazione moderna in quanto le sue applicazioni possono essere eseguite su diverse piattaforme, compresi i sistemi operativi Windows 10, iOS, Android e Macintosh. Inoltre, Microsoft Office può essere distribuito come applicazione nativa o anche come servizio SaaS. Tuttavia le applicazioni moderne presentano nuove sfide. Come potete proteggere e gestire le applicazioni moderne? Ad esempio, uno strumento di gestione client

tradizionale come SCCM consente di distribuire e gestire applicazioni desktop Windows legacy su un laptop con Windows 7, ma non consente di gestire le applicazioni moderne di Windows 10 su uno smartphone BYOD e di separare i dati personali del dipendente dai dati aziendali. Di conseguenza, è necessario integrare gli strumenti di gestione client tradizionali con la gestione della mobility aziendale (Enterprise Mobility Management, EMM). Questa combinazione di gestione client e EMM viene definita gestione unificata degli endpoint (Unified Endpoint Management, UEM).

### 3. Scomparsa del perimetro di sicurezza digitale

Con una forza lavoro maggiormente mobile è sempre più difficile conservare i dati aziendali nel datacenter. Gli utenti hanno bisogno di accedere ai propri file indipendentemente da dove questi si trovino, per esempio su un server protetto da un firewall, su un server in modalità hosted tramite un provider attendibile o sul desktop in ufficio. Alcuni dei vostri utenti potrebbero utilizzare client mobile nativi per la posta elettronica piuttosto che servizi virtuali, magari archiviando i file allegati alle e-mail sul proprio smartphone personale in un formato non cifrato. Allo stesso tempo, questi utenti potrebbero anche affidarsi a una VPN utilizzata da un hacker per accedere alle risorse oltre il firewall, tramite un'app mobile dannosa scaricata a insaputa del dipendente.

## Andate oltre la virtualizzazione e adottate un workspace digitale con Citrix

Un workspace digitale completo e integrato consentirà alle persone di accedere in modo sicuro ad applicazioni, desktop e dati da qualsiasi luogo. Citrix Workspace abbina la tecnologia di Citrix per la virtualizzazione ad altre funzionalità, tra cui l'UEM (Unified Endpoint Management), l'EFSS (Enterprise File Sync and Share), il gateway di accesso alla rete sicuro e Analytics per una sicurezza intelligente e un monitoraggio delle prestazioni delle applicazioni.

### Unified Endpoint Management (UEM)

L'UEM di Citrix semplifica la gestione da parte delle organizzazioni IT dei mobile workspace in continua crescita. Questa soluzione offre una gestione centralizzata su diverse piattaforme e dispositivi, inclusi desktop, laptop, smartphone, tablet, dispositivi IoT e altri thin client come i Chromebook di Google. Inoltre, Citrix vi consente di gestire non solo le applicazioni mobile, ma tutte le applicazioni moderne. Inoltre, solo con Citrix l'UEM offre funzionalità esclusive che aggiungono valore a Microsoft EMS/Intune, incluse le micro-VPN per Office 365. Sarete in grado di mantenere cifrati i dati sui dispositivi mobile, riducendo il problema della scomparsa del perimetro di sicurezza digitale.

#### Funzionalità principali dell'UEM di Citrix:

- Gestione dei dispositivi mobile (Mobile Device Management, MDM) sulle piattaforme più diffuse (tra cui Windows 10, iOS, Android, MacOS e IoT)
- Gestione flessibile delle applicazioni mobile (Mobile Application Management, MAM) con supporto per la piattaforma MAM (come l'applicazione gestita da iOS, Samsung KNOX, AppConfig Community o Windows Information Protection); Citrix MAM con tecnologia MDX che fornisce un secondo livello di crittografia a livello di applicazione senza registrazione del dispositivo; e supporto per Intune MAM per proteggere Office 365
- Applicazioni per una produttività sicura a livello aziendale, tra cui Secure Mail e Secure Web
- La gestione dei contenuti mobile (Mobile Content Management, MCM), inclusa la

tecnologia Citrix di sincronizzazione e condivisione dei file, si integra con Secure Mail che consente ai dipendenti di accedere ai file di lavoro ovunque, con un semplice clic su un link nella loro e-mail; inoltre elimina la necessità per gli utenti di inviare allegati con le e-mail

- Gestione dell'identità (Identity Management, IDM) con supporto per l'autenticazione a due fattori e il SSO per qualsiasi applicazione (mobile, virtuale, SaaS, web) fornita tramite un app store personalizzabile

- Sicurezza dell'accesso al gateway di rete con VPN micro-app esclusive, che riduce il rischio di accessi non autorizzati alla rete

### Sincronizzazione e condivisione di file aziendali (Enterprise File Sync and Share, EFSS)

Mentre la virtualizzazione del desktop e delle applicazioni consente agli utenti di accedere ai propri file da app virtuali, come notato in precedenza, sempre più utenti adottano app moderne e, pertanto, hanno bisogno di una soluzione completa e sicura per accedere ai propri file a prescindere dal tipo e dall'ubicazione delle app. L'EFSS di Citrix è una componente che si va ad integrare nella virtualizzazione del desktop e delle applicazioni per un mobile workspace completo.

#### L'EFSS di Citrix fornisce:

- L'accesso ai dati ovunque e su qualsiasi dispositivo tramite strumenti e applicazioni di sincronizzazione dei dati
- L'accesso sicuro ai dati all'interno della rete, compresi SharePoint e drive di rete
- Un'esperienza utente ottimizzata e conveniente con un plug-in per Microsoft Outlook® e l'integrazione in Windows Explorer e Mac Finder; il supporto di file di grandi dimensioni (fino a 100 GB); un editor integrato dei contenuti mobile
- Il controllo su dove risiedono i dati attraverso StorageZones e StorageZone Connectors per SharePoint e drive di rete, garantendo all'IT la flessibilità e il controllo necessari per poter archiviare i dati ovunque sia preferibile in termini di conformità alle normative, strategia dell'IT e infrastruttura

- Gestione e sicurezza centralizzate, con potenti funzionalità di reporting e di notifica, e l'integrazione di misure di DLP

- Policy di sicurezza del dispositivo di livello nativo per poter estendere la protezione agli endpoint

- La sincronizzazione on-demand per i desktop virtuali

### Citrix Unified Gateway

Con l'utilizzo di più tipi di dispositivi e applicazioni, è molto probabile che l'accesso remoto si complichino per l'IT, a causa di una miriade di altri prodotti specifici per i vari dispositivi, modelli di proprietà, reti e applicazioni. L'IT ha bisogno di consolidare e semplificare le infrastrutture di accesso remoto dando alle persone un modo semplice per accedere alle loro applicazioni da qualsiasi dispositivo.

Citrix Unified Gateway fornisce l'accesso remoto da qualsiasi tipo di dispositivo agli ambienti virtuali; l'accesso remoto SSL basato su VPN alle applicazioni aziendali, alle applicazioni web e SaaS; e l'integrazione con Citrix Unified Endpoint Management per l'accesso sicuro ai dispositivi mobile.

#### Citrix Unified Gateway fornisce anche:

- Un URL per accedere a qualsiasi applicazione utilizzando qualsiasi tipo di dispositivo, fornendo un accesso sicuro e unificato

- Funzionalità micro-VPN con l'UEM di Citrix per un accesso sicuro ai dispositivi mobile

- Un'esperienza con le applicazioni stabile e dalle prestazioni elevate, su qualsiasi rete

- Il single sign-on (SSO) alle applicazioni virtuali, mobile, web e SaaS

- L'autenticazione multi-fattore, il monitoraggio end-to-end di tutto il traffico applicativo e il controllo contestuale degli accessi

### Citrix Analytics

Utilizzando un ampio set di algoritmi di machine learning, Citrix Analytics offre funzionalità di sicurezza contestuale: correla e analizza i dati cross-product (dei diversi prodotti) per rilevare e isolare le attività rischiose degli utenti, siano esse originate da un dipendente interno o da un aggressore esterno malintenzionato.

Queste attività utente rischiose vengono combinate per creare un profilo di rischio aggregato per l'utente. Una volta identificate le attività rischiose per gli utenti, Citrix Analytics utilizza una serie di controlli granulari per attenuare la minaccia o per bloccarla completamente. Ad esempio, può abilitare l'autenticazione a più fattori, la registrazione delle sessioni utente, l'impostazione di soglie di accesso ai dati più rigide, il blocco delle applicazioni sospette e persino la messa in quarantena degli utenti.

#### Citrix Analytics:

- Fornisce un'analisi della sicurezza basata sul comportamento degli utenti che combina l'analisi della sicurezza degli accessi, delle applicazioni e dei dati

- Fornisce un'analisi delle prestazioni e delle operazioni per tenere traccia dell'utilizzo, per monitorare le prestazioni e per evidenziare i problemi e le cause principali

- Agisce in tempo reale a circuito chiuso modificando le policy del prodotto per ridurre le minacce

- Funziona in locale, su un cloud pubblico o su distribuzioni ibride

---

## Da dove cominciare

Molti clienti Citrix affrontano il passaggio a un workspace digitale optando per un'implementazione graduale che si concentra sulle specificità degli utenti e sui casi d'uso per la propria forza lavoro mobile. Avrete anche bisogno di individuare i principali casi d'uso e i flussi di lavoro. Considerateli dal punto di vista degli utenti e della forza lavoro, valutando anche le varie esigenze, preferenze e modalità di lavoro in base ai vari tipi di dispositivi, applicazioni e reti. La vostra valutazione dovrebbe includere anche i requisiti aziendali in termini di sicurezza e conformità. Molti di questi casi d'uso potrebbero essere legati a progetti attuali come la migrazione a Windows 10 o l'adozione di Office 365.

Quindi, teorizzate una soluzione delineando l'esperienza utente e i flussi di lavoro che vi proponete di raggiungere. Inizialmente concentratevi su obiettivi raggiungibili che possono offrire un rapido successo come l'adozione dell'UEM di Citrix per gestire i dispositivi Windows 10 e le applicazioni moderne insieme alla gestione di altri dispositivi e applicazioni. Oppure aggiungete l'EFSS di Citrix per supportare la condivisione avanzata dei file e ridurre la perdita di dati.

Il vostro "proof-of-concept" deve includere i rappresentanti di tutte le unità aziendali, per essere certi di soddisfare l'intero ventaglio delle loro esigenze. Implementa la vostra soluzione in locale, sul cloud o ibrida con un approccio graduale in base ai vostri utenti e ai casi d'uso identificati.

## Conclusioni

La diffusione di stili di lavoro mobili e di applicazioni moderne unita alla scomparsa del perimetro digitale costituisce una sfida che non può essere affrontata tramite la virtualizzazione o un insieme di tecnologie di più fornitori, in modo frammentario. Solo una soluzione di workspace completa e unificata può permettere alle persone di essere pienamente produttive su qualsiasi dispositivo, utilizzando qualsiasi applicazione, con un'esperienza di alta qualità e con la sicurezza richiesta dal reparto IT.

Un workspace dotato del supporto per una mobility completa consente al reparto IT di ottimizzare e semplificare. Lavorare con un unico fornitore per un workspace digitale completo consente di risparmiare tempo, riduce le esigenze di formazione del personale, semplifica il supporto tecnico, riduce i costi complessivi e offre agli utenti un'esperienza più conveniente e ottimizzata. Per migliorare il coinvolgimento e la produttività dei dipendenti, questi hanno bisogno di un workspace digitale che sia consapevole del contesto, affidabile e sufficientemente intelligente da offrire l'accesso, le informazioni e le prestazioni corretti per portare a termine il lavoro.

Grazie a Citrix Workspace le organizzazioni possono superare molti problemi legati alla sicurezza e alla gestione, fornendo un ricco insieme di applicazioni per la produttività mobile di livello enterprise, abilitando la condivisione sicura dei file su qualsiasi dispositivo e offrendo un'esperienza ottimizzata tramite una soluzione completa e integrata. Con l'implementazione di Citrix Workspace attraverso un approccio graduale basato sui principali casi d'uso, potete completare la transizione alla distribuzione di un workspace digitale e al contempo raggiungere un valore ottimale per la vostra azienda.

## Fasi successive

[Scoprite maggiori informazioni su Citrix Workspace](#)

[Fate il trade-up a Citrix Workspace e risparmiate](#)

## Fonti

<sup>1</sup> Gallup: State of the American Workplace, 2017



## Enterprise Sales

Dal Nord America | 800 424 8749

Dal resto del mondo | +1 408 790 8000

## Sedi

Sede centrale | 851 Cypress Creek Road Fort Lauderdale, Florida 33309, Stati Uniti

Silicon Valley | 4988 Great America Parkway Santa Clara, California 95054, Stati Uniti

© 2018 Citrix Systems, Inc. Tutti i diritti riservati. Citrix, il logo di Citrix e gli altri marchi citati nel presente documento sono di proprietà di Citrix Systems, Inc. e/o di una delle sue consociate, e potrebbero essere registrati presso l'Ufficio marchi e brevetti negli Stati Uniti e in altri Paesi. Tutti gli altri marchi sono di proprietà dei rispettivi proprietari.