



# Una strategia cloud ideale per l'azienda e per la forza lavoro

Utilizzate un workspace digitale integrato e in modalità hosted sul cloud per rendere gli utenti più produttivi, per semplificare l'IT e per garantire la sicurezza e l'agilità necessarie all'azienda





## Indice

Introduzione	3
Come semplificare l'IT nel modo giusto	4
Semplificare sia il lavoro che l'IT con un workspace digitale sicuro	5
Passare al cloud in modo più sicuro e intelligente	6
Aiutare le persone a diventare più produttive e coinvolte	7
Semplificare la gestione e la sicurezza degli endpoint	8
Aumentare l'agilità aziendale	9
Garantire la business continuity	10

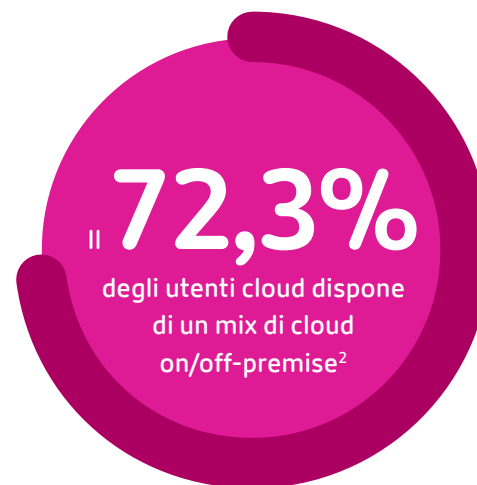
## Introduzione

Le persone non hanno mai avuto a disposizione così tanti modi per svolgere il proprio lavoro. I dispositivi e le applicazioni mobile consentono ai dipendenti di diventare produttivi ovunque, in qualsiasi momento. Questo è vantaggioso per l'azienda, ma complica la vita al reparto IT.

Abbiamo introdotto il SaaS, il cloud e la mobility, tuttavia le persone si affidano ancora alle applicazioni desktop di Windows, alle applicazioni web e alle applicazioni virtuali. Le aziende stanno trasferendo i carichi di lavoro e le applicazioni nel cloud, ma la maggior parte continuerà a utilizzare le risorse locali anche nel prossimo futuro.

All'aumentare delle opzioni a disposizione delle persone, cresce la diversità dell'ambiente aziendale. Contestualmente, per il reparto IT diventano più difficili le operazioni di protezione, provisioning, applicazione di patch, aggiornamento, riparazione e manutenzione di tutto il software e l'hardware utilizzato dalla forza lavoro.

Si può cadere nella tentazione di ridurre tutto questo a semplici ostacoli lungo il percorso verso il cloud e di pensare che una volta che si consolida tutto su un'unica piattaforma cloud, tutta questa complessità svanirà. L'IT ibrido e multi-cloud durerà a lungo con tutta probabilità, e questo aspetto è positivo. Dobbiamo soltanto trovare un modo efficace per gestire la complessità che ne deriva.



# Come semplificare l'IT nel modo giusto

Quando l'ambiente cresce e si diversifica, le organizzazioni IT sono oberate e spesso si rivolgono a soluzioni ad hoc per soddisfare le varie aree specifiche: gestione unificata degli endpoint (UEM), distribuzione delle applicazioni virtuali, enterprise mobility management (EMM), sicurezza della rete, gestione delle identità, condivisione di file e content collaboration, distribuzione delle applicazioni, sicurezza del cloud e così via. Ma la proliferazione degli strumenti aggiunge solo complessità, per non parlare dei costi, e la gestione diventa ancora più impegnativa.

Al contempo, più il reparto IT fatica a gestire tale complessità, maggiore è la possibilità che si verifichino lacune in termini di sicurezza e conformità, problemi di prestazioni e di business continuity, e altri imprevisti da affrontare. L'azienda, che sperava di ottenere una rinnovata agilità nel cloud, si trova invece rallentata da tecnologie basate su silos, da una gestione disorganica e da un'esperienza utente frustrante e frammentata.

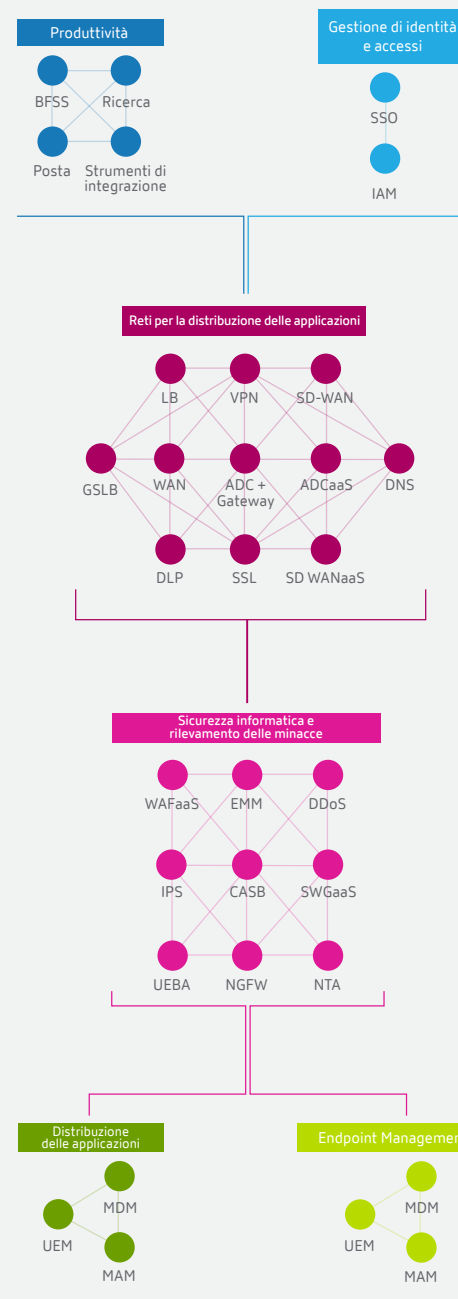
Le soluzioni ad hoc non sono una risposta adeguata alla crescente complessità. Per distribuire tutte le applicazioni necessarie alla forza lavoro dinamica e mobile di oggi, senza essere sommersi da conseguenze indesiderate, è auspicabile che le aziende adottino workspace digitali sicuri, integrati e basati sul cloud.

Con un workspace digitale sicuro, potete:

- Offrire ai dipendenti un'esperienza ottimizzata, omogenea e coinvolgente
- Ridurre i costi dell'IT e semplificarne la gestione
- Adottare un approccio olistico alla sicurezza e alla conformità, colmando al contempo le lacune
- Aiutare l'azienda a mantenere il massimo livello di agilità

**L'83%** delle organizzazioni afferma che la complessità delle loro strutture organizzative e dell'infrastruttura IT li mette ancora più a rischio di violazioni della sicurezza.<sup>3</sup>

## Prodotti di nicchia = complessità

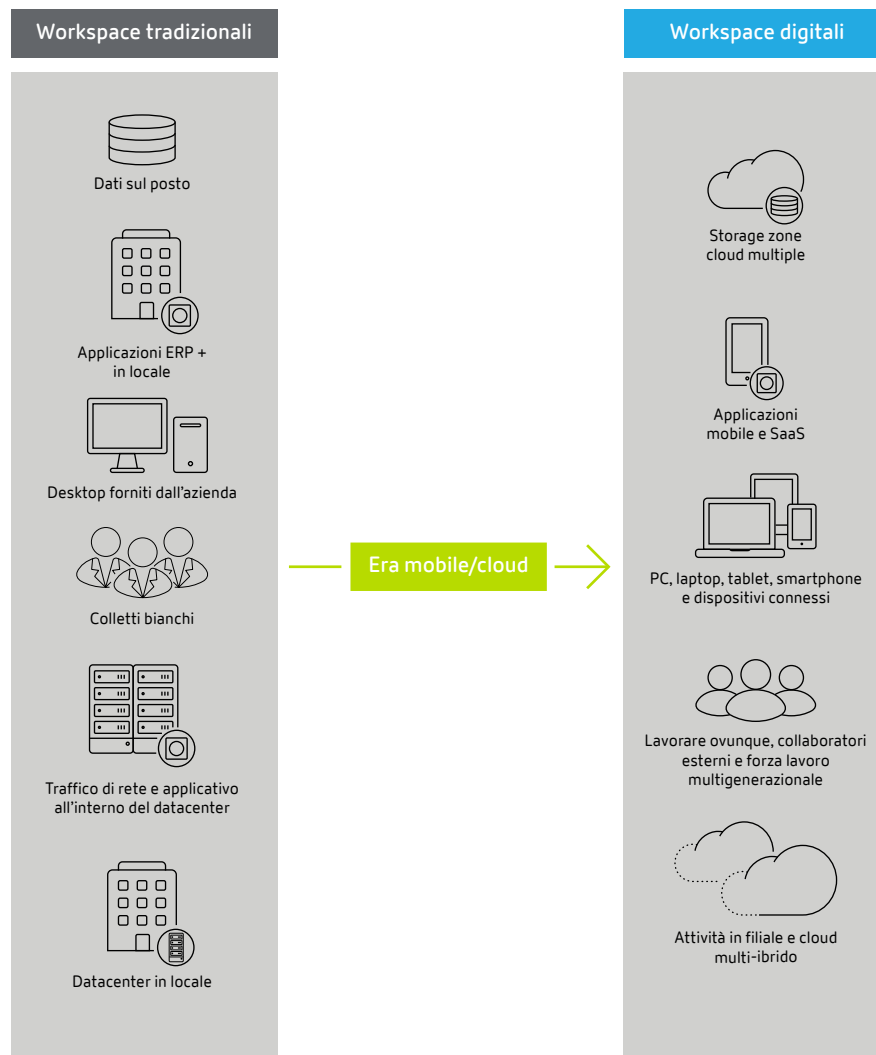


# Semplificare sia il lavoro che l'IT con un workspace digitale sicuro

Un workspace digitale offre un luogo specifico tramite cui le persone possono accedere in modo sicuro a tutte le applicazioni, i desktop e i dati, da qualsiasi luogo. I dipendenti godono di un'esperienza ottimizzata di single sign-on, indipendentemente da come o dove lavorano, e ciò comprende:

- Qualsiasi dispositivo
- Qualsiasi cloud
- Qualsiasi rete
- Qualsiasi tipo di applicazione (cloud/SaaS, web, mobile e Windows)

Il reparto IT ottiene una sicurezza e un controllo unificati nel back-end, senza il costo e la complessità legati a una miriade di soluzioni ad hoc. Le tecnologie complementari, tra cui la sicurezza dei dispositivi, la sincronizzazione e condivisione sicura dei file, la sicurezza della rete e gli analytics intelligenti, aiutano a rafforzare la sicurezza. Al contempo, gli analytics basati sugli utenti mettono in evidenza i rischi potenziali e le aree dove è possibile apportare miglioramenti a livello operativo.

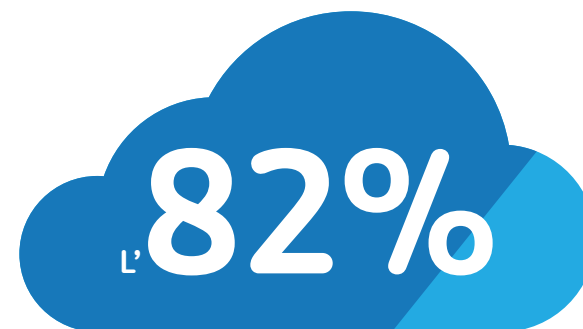


## Passare al cloud in modo più sicuro e intelligente

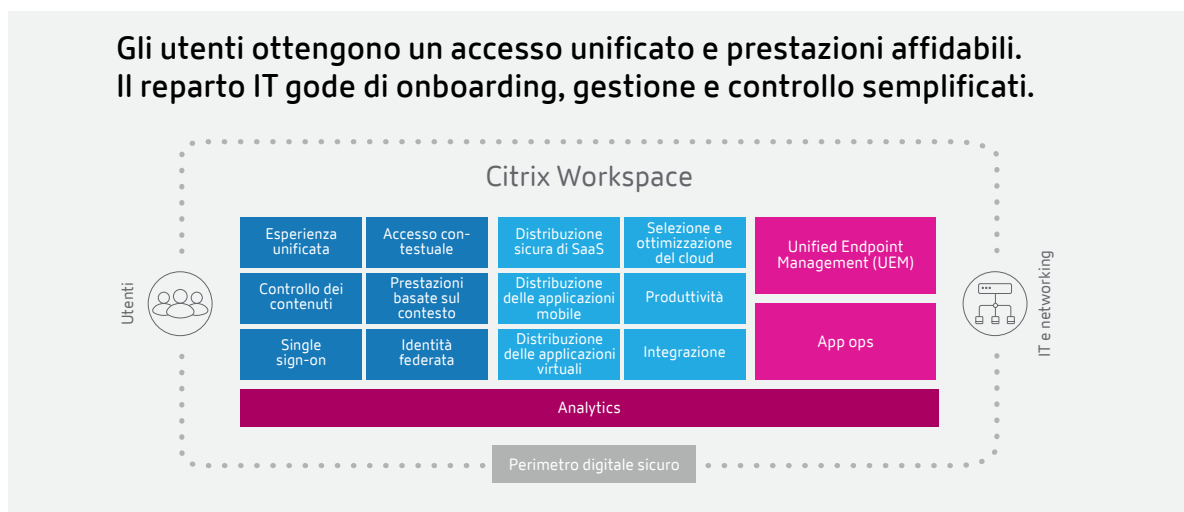
La sicurezza è sempre una preoccupazione per le aziende che spostano i carichi di lavoro sul cloud o che utilizzano il SaaS o le applicazioni web. Uscendo dal datacenter si ha la sensazione di perdere il controllo e spesso è proprio così.

Un workspace digitale sicuro garantisce che le aziende abbiano il controllo. Il reparto IT dispone così di un singolo posto da cui monitorare e controllare l'accesso a tutti i servizi cloud utilizzati dai dipendenti, incluse le applicazioni adottate di propria iniziativa ma non esplicitamente autorizzate. Grazie a funzionalità di controllo come la creazione di blacklist/whitelist e l'applicazione di watermark per categorie di URL e siti web specifici, nonché la possibilità di limitare le funzionalità di copia/incolla e download, il reparto IT può gestire i rischi in modo efficace. Un browser sicuro all'interno del workspace protegge le persone che hanno inavvertitamente fatto clic su un collegamento non sicuro in un documento o all'interno di un'applicazione come Salesforce. I dati possono essere crittografati e protetti ovunque si trovino (archiviati su un dispositivo, sul cloud o in transito). Per le applicazioni e i servizi web, la sicurezza e i firewall a livello di applicazione scoraggiano gli exploit zero-day e gli attacchi DDoS.

Oltre a ridurre i rischi legati all'adozione del servizio cloud, un workspace digitale sicuro aiuta il reparto IT anche a garantire che il proprio budget venga speso nel modo migliore possibile. Per prendere decisioni di investimento più intelligenti e utilizzare nel modo migliore le risorse tecnologiche aziendali, le aziende possono sfruttare la visibilità, i dati e gli analytics unificati delle risorse maggiormente utilizzate e delle rispettive performance.



ritiene che la capacità della propria organizzazione di migrare le applicazioni nel cloud sia ostacolata dalla maggiore complessità dell'infrastruttura di rete<sup>2</sup>



## Aiutare le persone a diventare più produttive e coinvolte

Dover gestire un processo di autenticazione diverso per ogni risorsa a cui si accede o cambiare il modo di lavorare in base al tipo di dispositivo o applicazione utilizzati, rende il lavoro complicato.

Con un workspace digitale sicuro, il reparto IT può offrire ai dipendenti un'esperienza ottimizzata indipendentemente dal tipo di dispositivo utilizzato, che comprende:

- Il single sign-on a tutte le applicazioni, di qualsiasi tipo, tramite un singolo URL
- Il roaming di sessione in modo che le persone possano aprire un'applicazione su un dispositivo, per poi proseguire a lavorare su un altro dispositivo, riprendendo esattamente da dove avevano interrotto
- Un unico posto dove trovare e accedere a tutti i file (a prescindere se si trovino su server di file aziendali, Microsoft SharePoint o archivi di file pubblici o privati), utilizzando qualsiasi dispositivo

Semplificare lo svolgimento del lavoro per le persone è ovviamente positivo per l'azienda. Così come è positivo disporre di una forza lavoro più impegnata, coinvolta e soddisfatta. Quando le persone hanno gli strumenti necessari per svolgere il proprio lavoro nel modo migliore, l'intera organizzazione è più stimolata e diventa più innovativa e produttiva. L'azienda diventa anche più attraente per i migliori talenti e le persone desiderano lavorare e rimanere lì più a lungo. Questo è un grande vantaggio in un settore con un elevato turnover e una concorrenza spietata per accaparrarsi i migliori dipendenti.



Le aziende che beneficiano del coinvolgimento dei dipendenti superano del

# 202%<sup>4</sup>

quelle che non sfruttano questo vantaggio

## Semplificare la gestione e la sicurezza degli endpoint

Con così tanti PC, laptop, smartphone, tablet e dispositivi IoT nell'ambiente aziendale, la sensazione degli amministratori IT è quella di collegarsi di continuo a una console di gestione dei dispositivi dopo l'altra. Questo fa perdere tempo e rende difficile mantenere una coerenza nell'applicazione delle policy, specialmente quando gruppi diversi gestiscono tipi di endpoint diversi. E la diversità dei dispositivi non farà che crescere, di pari passo con l'evoluzione dell'IoT.

Un workspace digitale sicuro semplifica la gestione degli endpoint consentendo di utilizzare un'unica console per applicare un framework di policy comune a tutte le risorse, indipendentemente dal tipo di dispositivo, applicazione, sistema operativo o rete. Gli amministratori ottengono una visibilità completa e il controllo sull'accesso degli utenti, e questo li aiuta a proteggere i contenuti e le applicazioni SaaS, web e mobile, a prescindere da come o dove vengono utilizzati.



Si stima che nel 2020 il numero di dispositivi connessi alla rete sarà pari a 6,58 a persona, che tradotto significa circa

# 50 miliardi

di dispositivi connessi in totale<sup>5</sup>





## Aumentare l'agilità aziendale

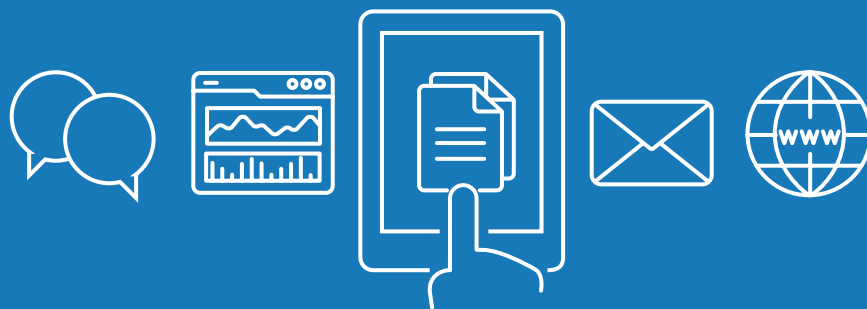
I processi tradizionali per l'onboarding dei dipendenti e l'apertura delle filiali rappresentano un modello di inefficienza. Gli amministratori creano le immagini di un desktop standard approvato con le applicazioni adatte, scaricano l'immagine sul desktop o sul laptop e poi aspettano che il dipendente lo ritiri fisicamente presso l'ufficio, oppure lo impacchettano e glielo spediscono. Gli aggiornamenti futuri delle applicazioni seguono un processo simile. Tale approccio, dispendioso in termini di tempo e lavoro, rallenta l'impatto delle assunzioni più importanti e delle iniziative strategiche.

Con un workspace digitale sicuro, i dipendenti possono acquistare qualsiasi tipo di dispositivo desiderino e accedere alla rete aziendale per eseguire automaticamente il provisioning delle applicazioni approvate dall'azienda, preconfigurate con i giusti controlli di sicurezza. L'azienda, che è in grado di espandersi e crescere in modo più efficiente e sicuro, può beneficiare di una migliore agilità aziendale proprio grazie al cloud.

## Garantire la business continuity

Rispondere a un'emergenza (per fenomeni naturali, sociali, informatici o in caso di cyber attacco) può essere un processo lento e caotico. Se la vostra strategia dipende dall'acquisizione e configurazione di più PC, e quindi dalla loro distribuzione agli utenti impossibilitati a raggiungere l'ufficio, potete perdere ore o giorni critici di business continuity e produttività.

Grazie a un workspace digitale sicuro, le persone possono accedere a tutte le loro applicazioni e ai dati utilizzando il proprio PC di casa, il laptop o anche lo smartphone, con la stessa esperienza a cui sono abituati e che avrebbero in ufficio. La capacità di continuare a lavorare senza perdere tempo, dati o contatti di collaborazione con i propri team, non solo consente di mandare avanti l'attività, ma può anche aiutare le persone a sentirsi al sicuro e a mantenere la situazione sotto controllo durante la fase di recupero dall'interruzione.





## Aumentare l'agilità aziendale

I processi tradizionali per l'onboarding dei dipendenti e l'apertura delle filiali rappresentano un modello di inefficienza. Gli amministratori creano le immagini di un desktop standard approvato con le applicazioni adatte, scaricano l'immagine sul desktop o sul laptop e poi aspettano che il dipendente lo ritiri fisicamente presso l'ufficio, oppure lo impacchettano e glielo spediscono. Gli aggiornamenti futuri delle applicazioni seguono un processo simile. Tale approccio, dispendioso in termini di tempo e lavoro, rallenta l'impatto delle assunzioni più importanti e delle iniziative strategiche.

Con un workspace digitale sicuro, i dipendenti possono acquistare qualsiasi tipo di dispositivo desiderino e accedere alla rete aziendale per eseguire automaticamente il provisioning delle applicazioni approvate dall'azienda, preconfigurate con i giusti controlli di sicurezza. L'azienda, che è in grado di espandersi e crescere in modo più efficiente e sicuro, può beneficiare di una migliore agilità aziendale proprio grazie al cloud.

## Garantire la business continuity

Rispondere a un'emergenza (per fenomeni naturali, sociali, informatici o in caso di cyber attacco) può essere un processo lento e caotico. Se la vostra strategia dipende dall'acquisizione e configurazione di più PC, e quindi dalla loro distribuzione agli utenti impossibilitati a raggiungere l'ufficio, potete perdere ore o giorni critici di business continuity e produttività.

Grazie a un workspace digitale sicuro, le persone possono accedere a tutte le loro applicazioni e ai dati utilizzando il proprio PC di casa, il laptop o anche lo smartphone, con la stessa esperienza a cui sono abituati e che avrebbero in ufficio. La capacità di continuare a lavorare senza perdere tempo, dati o contatti di collaborazione con i propri team, non solo consente di mandare avanti l'attività, ma può anche aiutare le persone a sentirsi al sicuro e a mantenere la situazione sotto controllo durante la fase di recupero dall'interruzione.

## La business continuity<sup>e</sup> il ripristino di emergenza sono in cima alla lista dei più importanti progetti tecnologici ai quali i reparti IT stanno attualmente lavorando<sup>6</sup>.



Mentre i moderni ambienti IT ibridi e multi-cloud diventano più complessi, un workspace digitale sicuro consente di offrire ai lavoratori un'esperienza migliore rafforzando la sicurezza e semplificando l'IT, in modo che l'azienda possa ottenere un maggiore valore in ogni fase del proprio percorso verso il cloud.

Se siete interessati a esplorare i vantaggi potenziali di un workspace digitale sicuro per la vostra organizzazione, vi invitiamo a scoprire di più su Citrix Workspace al seguente indirizzo:

[citrix.it/products/citrix-workspace/](https://citrix.it/products/citrix-workspace/)

Fonte:

1. report "IDG Cloud Insights 2018".
2. Come si stanno preparando le organizzazioni per garantire la distribuzione delle applicazioni in un ambiente multi-cloud? IDC Infobrief, ottobre 2017.
3. "The Need for a New IT Security Architecture", Ponemon Institute, sponsorizzato da Citrix nel 2017.
4. "Remote Workforce NPS: The Most Important Metric You're Missing", Business 2 Community, marzo 2017.
5. "Number of network connected devices per person around the world from 2003 to 2020", Statista.com.
6. CIO Tech Poll: Tech Priorities 2018, IDG.

