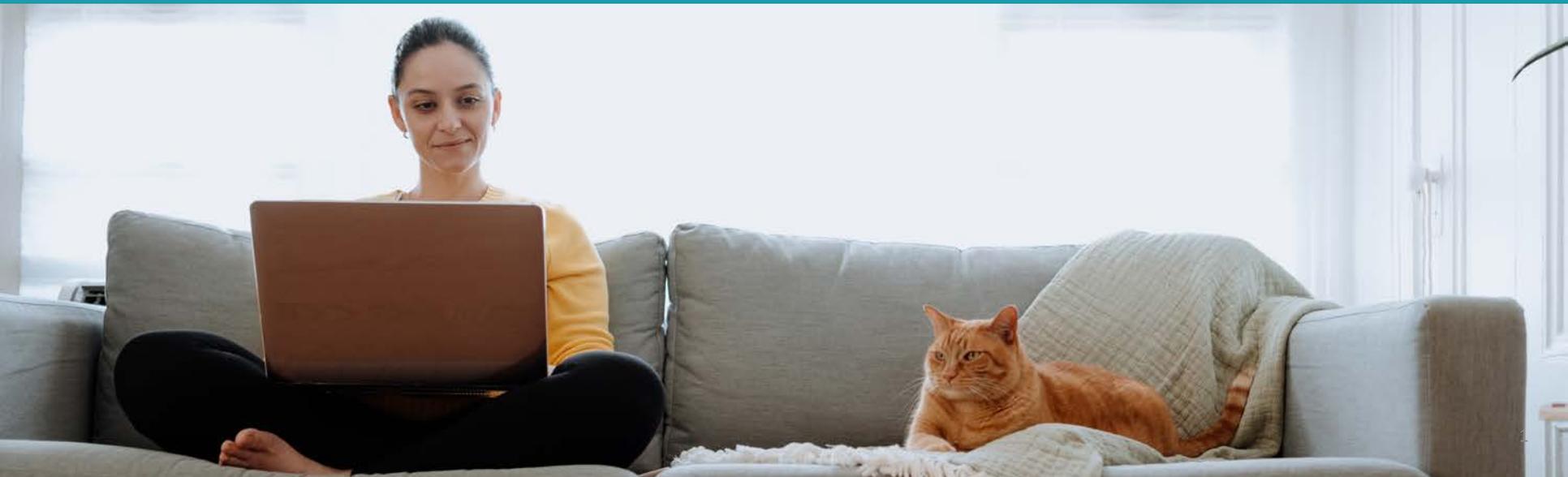


# Tre modi in cui il workspace digitale avvantaggia sia i dipendenti che il reparto IT.



Il lavoro remoto è un trend in crescita già da vari anni. Ma quasi dall'oggi al domani, il numero di persone che lavora da casa è più che raddoppiato a causa del Covid-19. Di conseguenza, le aziende prive di un piano di lavoro remoto affidabile hanno dovuto darsi da fare per implementarne uno. Non è facile mantenere le aziende aperte e garantire che siano redditizie, fornire ai dipendenti gli strumenti necessari per lavorare in remoto, assicurare che i dipendenti rimangano coinvolti e produttivi e proteggere le informazioni sensibili con un breve preavviso.



# Un cambio di mentalità sul lavoro remoto

In passato, molte aziende si sono opposte al lavoro remoto per vari motivi. Alcune aziende e i rispettivi manager erano preoccupati che i dipendenti, lavorando da remoto, non avrebbero mantenuto un livello di produttività adeguato o che la collaborazione potesse essere penalizzata. Altri temevano una crescita dei rischi per la sicurezza.

Tuttavia, molte di queste aziende ora adottano il lavoro remoto: hanno scoperto che effettivamente può funzionare bene, che offre vantaggi tangibili come la business continuity e che consente di mantenere livelli elevati di collaborazione, produttività e sicurezza.

## Più lavoro remoto significa più lavoro per i reparti IT

+/- 5 mln

Numero di dipendenti americani che hanno lavorato da casa part-time prima della pandemia

42 mln

Numero di dipendenti americani che probabilmente lavoreranno da casa entro la fine del 2021

733%

Percentuale di incremento potenziale del lavoro remoto in meno di due anni

Prima di adottare il lavoro remoto, ci sono alcune importanti domande relative all'implementazione che i dirigenti dovrebbero porsi. Nello specifico:

Per i reparti IT, quanto è difficile supportare una forza lavoro distribuita in ambienti remoti, in locale e ibridi? E in che modo le aziende si assicurano di disporre della tecnologia adeguata per consentire il lavoro remoto senza ostacoli digitali e rischi per la sicurezza?

Gli esperti stimano che, prima della pandemia, il 3,6% (vale a dire circa 5 milioni) dei dipendenti americani lavorava da casa almeno 2 o 3 giorni alla settimana, sebbene i sondaggi mostrassero che fino all'80% dei dipendenti desiderava lavorare da casa. Questi stessi esperti stimano che entro la fine del 2021 il numero degli americani che lavorano da casa potrebbe raggiungere il 30% (circa 42 milioni di persone).

# La potenza del workspace digitale soddisfa la domanda di lavoro remoto

Fornire un'esperienza utente eccezionale, sicura e remota è più semplice e può essere più conveniente rispetto a quanto ipotizzato dalle aziende. Richiede semplicemente la tecnologia giusta: un workspace digitale sicuro. Coloro che possono trarre vantaggio da un'esperienza utente eccezionale non sono solo i dipendenti remoti, ma anche quelli che lavorano fuori sede o che si trovano in una condizione ibrida.

# Una panoramica del workspace digitale sicuro

**Di seguito troverete i tre modi principali in cui un workspace digitale sicuro avvantaggia allo stesso modo i dipendenti e i professionisti IT:**

## Unifica le soluzioni IT

- Centralizza lo storage di applicazioni e dati
- Semplifica la gestione dell'intero ecosistema tramite una singola piattaforma
- Assicura single sign-on e accessi semplificati a tutti i file, i dati e le applicazioni da qualsiasi luogo
- Consente di avvalersi di microapp personalizzabili che facilitano l'adattamento delle attività alle esigenze individuali
- Ottimizza le attività ripetitive grazie a flussi di lavoro intelligenti
- Fornisce un'esperienza ottimizzata su ogni dispositivo

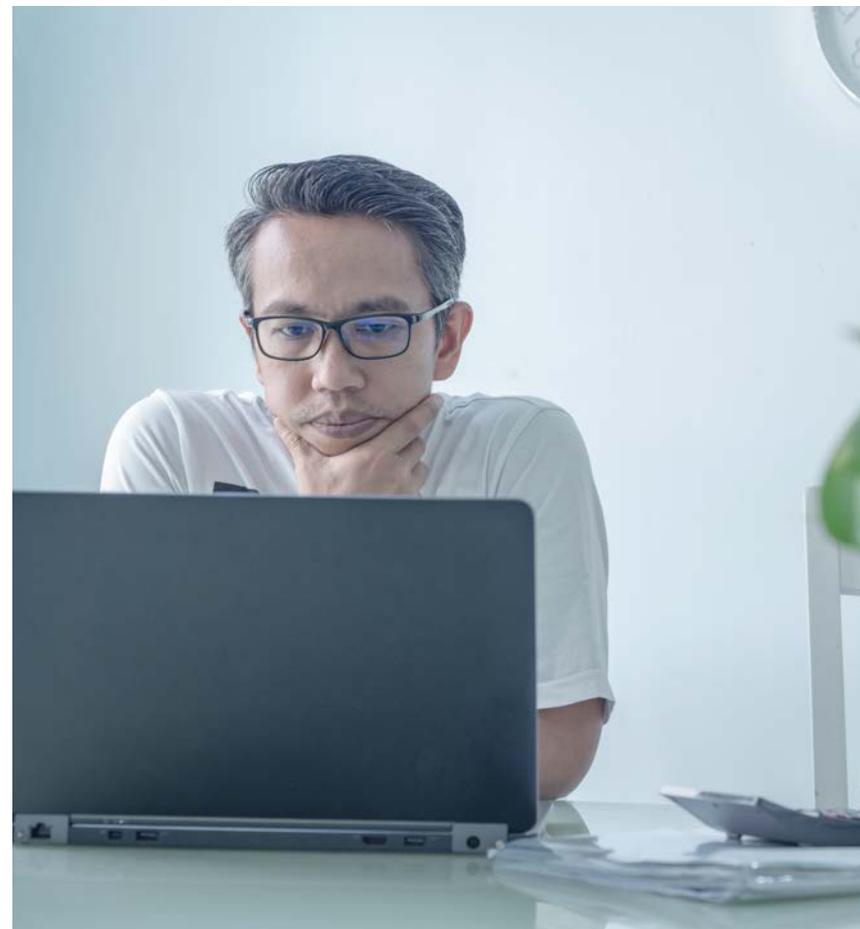
## Protegge il vostro ecosistema

- Offre agli amministratori un controllo a livello granulare
- Contestualizza i comportamenti e visualizza l'attività su applicazioni, cloud e reti
- Diminuisce la tendenza a ricorrere ad applicazioni e download non autorizzati
- Aiuta il reparto IT a individuare anomalie e trend in modo da poter ottimizzare gli strumenti utilizzati dai dipendenti per migliorare le prestazioni e aumentare la produttività
- Assicura la visibilità su applicazioni, reti, cloud e dispositivi

## Fornisce analytics per insight azionabili

- Semplifica il monitoraggio e l'identificazione di attività insolite sulla rete
- Migliora la comprensione dei comportamenti e delle esigenze degli utenti per garantire la soddisfazione dei dipendenti e mantenere tassi di adozione elevati
- Aiuta a ottimizzare le prestazioni delle applicazioni
- Supporta la ricerca e la risoluzione dei problemi relativi alle prestazioni di rete più velocemente
- Mette in evidenza le connessioni lente e semplifica il reindirizzamento rapido del traffico

Nelle seguenti pagine, esamineremo questi vantaggi più nel dettaglio.



# 1. Una soluzione IT unificata per un connubio perfetto

I dipendenti hanno vari tipi di esigenze. Ad esempio, persone o team diversi potrebbero necessitare di applicazioni, dispositivi o diritti di accesso specifici. Una soluzione flessibile a volte può richiedere di sacrificare l'esperienza utente o il controllo da parte del reparto IT. Soddisfare tutte le varie esigenze può rappresentare una sfida, a meno che non si disponga di una soluzione unificata in grado di offrire esperienze eccezionali e, al contempo, capace di soddisfare le esigenze specifiche dei diversi team e individui.

## I dipendenti desiderano un accesso semplice alle applicazioni e ai dati

Quando distribuite un workspace digitale unificato, ai dipendenti basta eseguire il login solo una volta per accedere alle applicazioni, ai file e ai dati di cui hanno bisogno, ovunque. Inoltre, grazie al workspace possono trovare più facilmente le informazioni che stanno cercando, ottimizzando la giornata lavorativa e migliorando l'esperienza.

Fonti: <sup>1</sup><https://www.willistowerswatson.com/en-US/Insights/2020/06/after-covid-19-cyber-and-the-coming-remote-work-revolution>

<sup>2</sup>[https://www.workfront.com/sites/default/files/resource/file\\_pdf/2019-09/sow-report-2020.pdf](https://www.workfront.com/sites/default/files/resource/file_pdf/2019-09/sow-report-2020.pdf)

# 37%

Percentuale dei dipendenti intervistati che concorda fermamente sul fatto che le applicazioni e i dispositivi forniti dalla propria organizzazione danno un contributo positivo all'esperienza lavorativa dei dipendenti.<sup>1</sup>

The Economist Intelligence Unit

# 71%

Percentuale dei dipendenti che vorrebbe disporre di un'unica destinazione per le informazioni e la gestione del lavoro. Tuttavia, secondo un recente studio di Workfront, una percentuale quasi uguale (il 69%) afferma di non disporre di una simile soluzione.<sup>2</sup>

# Offrite a tutti ottime esperienze

**Le esigenze dei dipendenti non sempre coincidono con quelle dei professionisti IT. Diamo uno sguardo a come la tecnologia giusta soddisfa le necessità di chiunque:**

## Esperienze eccezionali per i dipendenti

- Uno spazio digitale intelligente che ottimizza i flussi di lavoro e promuove la collaborazione
- Tutte le applicazioni e i dati SaaS in un unico posto per ridurre al minimo lo switching dei contenuti e favorire la concentrazione
- Assicura single sign-on e accessi semplificati a tutti i file, i dati e le applicazioni da qualsiasi luogo
- Esperienze ottimizzate su tutti i dispositivi, i cloud e le reti
- Un modo semplice per eseguire l'onboarding e l'offboarding dei dipendenti, ovunque
- Automazione delle attività di routine
- Una connessione sicura ai dati aziendali

## Esperienze eccezionali per i professionisti IT

- Un modo semplice per fornire un accesso sicuro e ottimizzato ad applicazioni e dati su vari dispositivi, cloud e reti
- Gestione unificata di applicazioni, dati e dispositivi tramite una singola piattaforma
- Possibilità di cancellare da remoto i dispositivi smarriti o rubati
- Insight basati sui dati per una risoluzione dei problemi più semplice e per migliorare velocità e prestazioni
- Microapp personalizzabili che vi consentono di adattare gli strumenti a team, ruoli ed esigenze individuali specifici



“

**Il nostro obiettivo è fornire una piattaforma di lavoro unificata, sicura e intelligente che trasformi l'esperienza dei dipendenti organizzando, gestendo e automatizzando tutte le attività che le persone devono svolgere al meglio.”**

---

**Calvin Hsu,**  
Vice President, Product Management, Citrix

# Riducete al minimo lo switching dei contenuti

**Molte organizzazioni ancora ritengono che i dipendenti debbano recarsi in ufficio per essere produttivi. Tuttavia, uno degli aspetti che più penalizzano la produttività non è affatto la posizione, ma è lo switching dei contenuti, vale a dire il passaggio da un'attività a un'altra, o tra varie applicazioni, software e altre soluzioni.**

Una soluzione in grado di consolidare tutti gli strumenti necessari ai dipendenti in un'unica piattaforma di facile utilizzo rappresenta una rivoluzione per la produttività. Consente di lavorare in modo innovativo e di migliorare la definizione delle priorità, con un conseguente aumento della produttività per tutti i dipendenti, compresi i professionisti IT.

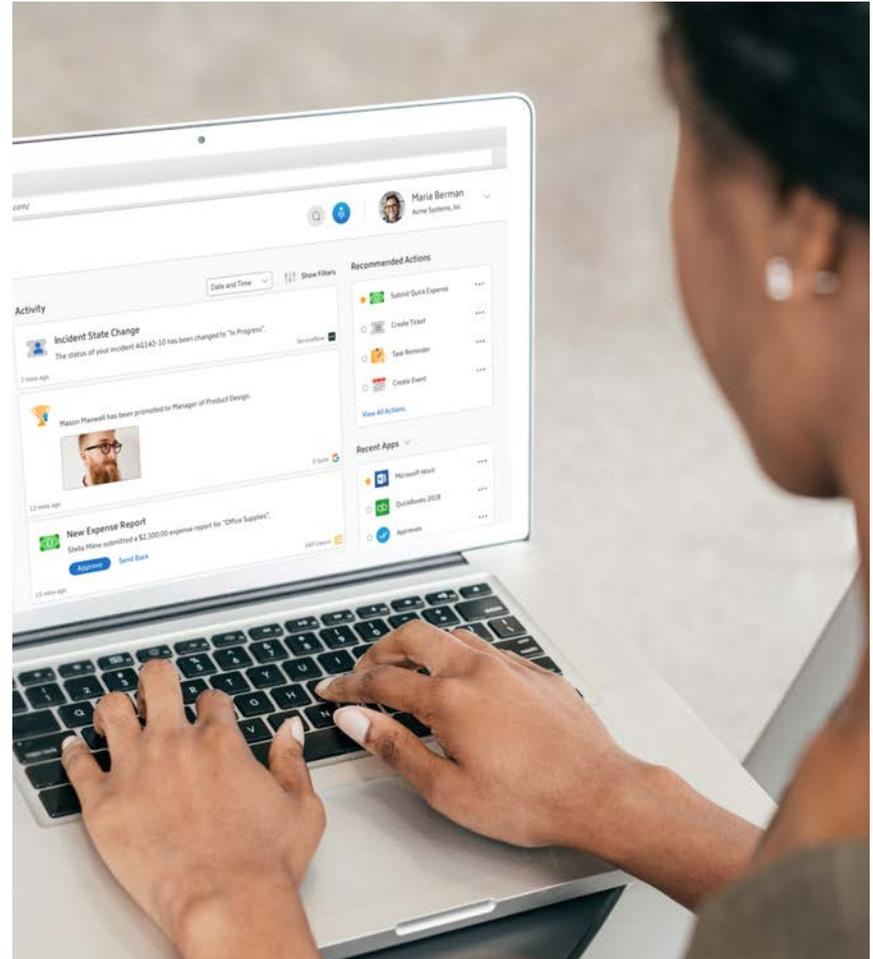
Fonte: <sup>1</sup><https://www.psychologytoday.com/us/blog/brain-wise/201209/the-true-cost-multi-tasking>

**-40%**

Il calo di produttività che può derivare da uno switching delle applicazioni eccessivo.<sup>1</sup>

# Create le condizioni per flussi di lavoro intelligenti

Quando le soluzioni vengono consolidate su una singola piattaforma, come un workspace digitale, possono dialogare tra loro e attingere alle informazioni di tutte le applicazioni e file. Il workspace digitale può quindi mettere in risalto le applicazioni più comunemente utilizzate nella parte superiore del feed degli utenti finali, inviare notifiche per ricordare loro le attività imminenti, automatizzare le attività di routine e semplificare i flussi di lavoro per mettere a portata di mano tutto il necessario.



Fonte: <sup>1</sup> - American Psychological Association

## Stimolate la concentrazione con microapp personalizzabili

**Anche se la maggior parte delle volte utilizzano solo una o due funzionalità, i dipendenti devono comunque accedere a un'applicazione e navigare in tutta l'interfaccia. Nel lungo termine questo si traduce in un'enorme perdita di tempo e in un ostacolo alla produttività.**

Ma quando i dipendenti dispongono di un workspace digitale con microapp personalizzate, possono occuparsi rapidamente delle piccole attività di routine in modo da poter continuare a lavorare senza interruzioni.

Un workspace digitale unificato semplifica il compito del reparto IT consentendo di:

- Personalizzare le microapp per offrire ai dipendenti un rapido accesso alle funzionalità necessarie
- Avviare integrazioni pronte all'uso che semplificano la distribuzione di microapp
- Creare microapp in pochi minuti, non in alcuni mesi



## 2. Una sicurezza completa per l'intero ecosistema

Gli attacchi informatici e le violazioni sono aumentati paurosamente a seguito della pandemia e dell'aumento del lavoro remoto. I motivi sono vari. Innanzitutto, il repentino aumento della navigazione, degli acquisti, delle spese e della condivisione di dati sensibili online ha consentito ai criminali informatici di avere un maggiore accesso ai dati.

In secondo luogo, molte organizzazioni, spinte dalla fretta di svolgere il proprio lavoro abituale, hanno dovuto adottare scorciatoie in termini di sicurezza per mantenere operativi i dipendenti.

# 273%

I crimini informatici stanno costando caro alle aziende. Nel primo trimestre di quest'anno le violazioni dei dati su larga scala sono aumentate del 273% rispetto allo stesso periodo dell'anno scorso<sup>1</sup>

*Fonte:* <sup>1</sup><https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html>

## Le minacce in numeri

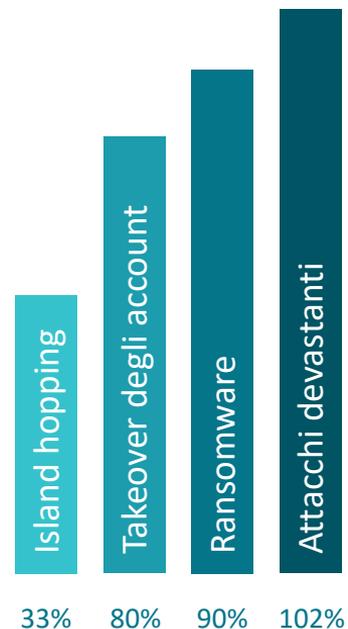
Le minacce informatiche sono in aumento in ogni ambito. In un contesto dominato dal caos causato dalla pandemia di coronavirus, gli hacker hanno scoperto che rubare dati e denaro è più facile che mai. Molte grandi aziende sono cadute vittime degli attacchi e i costi possono essere notevoli.

Gli attacchi di tipo “island hopping” sono cresciuti del 33%

I tentativi per cercare di impadronirsi degli account sono aumentati dell’80%

Il ransomware è cresciuto del 90%

Gli attacchi devastanti sono cresciuti del 102%

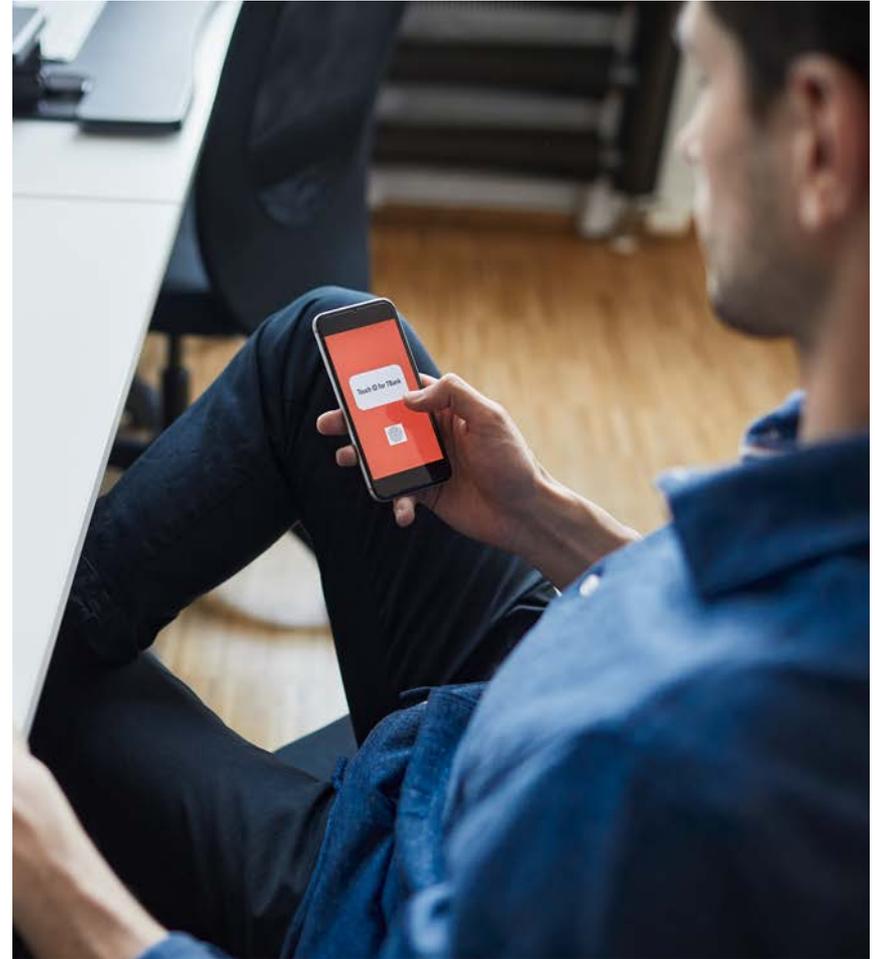


L’aumento degli attacchi nel 2020, secondo un rapporto della CNBC.<sup>1</sup>

Fonte: <sup>1</sup><https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html>

## Le misure di sicurezza di base non sono sufficienti

Alcune organizzazioni si sono affidate a soluzioni come le VPN per fornire ai dipendenti un tunnel sicuro per i dati aziendali, tuttavia queste soluzioni oltre a non essere complete non sono neanche ideali. Nello specifico, per i reparti IT le VPN diventano rapidamente complesse da gestire, non sono progettate per un utilizzo elevato, sono facili bersagli per le minacce informatiche e non sono versate per la privacy o per gli utenti.





“

**I lavoratori remoti sono anche bombardati da attacchi basati su tematiche legate alla crisi del Covid-19 che traggono vantaggio dai ritardi negli aggiornamenti di e-mail e filtri web e che utilizzano l'ingegneria sociale per approfittarsi delle preoccupazioni della forza lavoro.”**

---

McKinsey

# Trovate il giusto equilibrio fra sicurezza ed efficienza

**Un workspace digitale sicuro aiuta le organizzazioni a ridurre al minimo i costi aggiuntivi per la sicurezza. Cercate una soluzione che integri sistemi di sicurezza al suo interno.**

**Dovrebbe includere funzionalità come:**

- **Storage dei dati e accessi centralizzati:** offrite ai dipendenti un facile accesso alle informazioni necessarie. In questo modo non ricorreranno a soluzioni alternative non autorizzate creando problemi di Shadow IT
- **Visibilità approfondita e controlli di livello granulare:** consentite al reparto IT di concedere o limitare gli accessi in base alle necessità, proteggendo i dati da coloro che non dovrebbero avervi accesso
- **BYOD e approcci orientati al mobile:** assicuratevi che i dipendenti abbiano un accesso sicuro su qualsiasi dispositivo
  - ~ Sia che si tratti di dispositivi di proprietà aziendale o personale
  - ~ Su reti non sicure
  - ~ Con la possibilità di cancellare da remoto i dati se un dispositivo viene smarrito o rubato

- **Un modello di sicurezza Zero Trust:** monitorate continuamente tutte le entità (come utenti, dispositivi, applicazioni, reti e API) e, di contro, offrite ai dipendenti maggiore libertà di svolgere il proprio lavoro da postazioni remote
- **Automazione delle attività comuni:** semplificate l'orchestrazione e l'automazione delle attività comuni per i reparti IT, come le attività di risposta agli incidenti, per ridurre al minimo le probabilità di sviste e errori umani, liberando al contempo risorse per il monitoraggio attivo delle minacce

## Compensate i costi legati alla protezione dei dati

Gli investimenti in misure di sicurezza individuali o frammentarie comportano l'aumento dei costi IT. Un modo per ridurre i costi di protezione dei dati consiste nell'implementare una soluzione IT completa che integri la sicurezza al suo interno.

Fonte: <sup>1</sup> <https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets>

+/- 70%

dei CISO e di chi acquista sistemi di sicurezza ritiene che i budget si ridurranno entro la fine del 2020, ma prevede di chiedere aumenti significativi nel 2021.<sup>1</sup>

### 3. Analytics per insight basati sui dati

Quando le aziende iniziano a passare da framework di lavoro remoto implementati frettolosamente a strategie IT lungimiranti, gli analytics diventano un componente necessario per supportare gli obiettivi aziendali. Forniscono insight sui dati, basati sugli utenti, relativi ai cambiamenti in atto all'interno dell'organizzazione. In questo modo, i reparti IT possono prendere decisioni informate, ottimizzare l'ambiente per una migliore esperienza dei dipendenti, individuare rapidamente le anomalie di sicurezza e agire rapidamente laddove necessario.

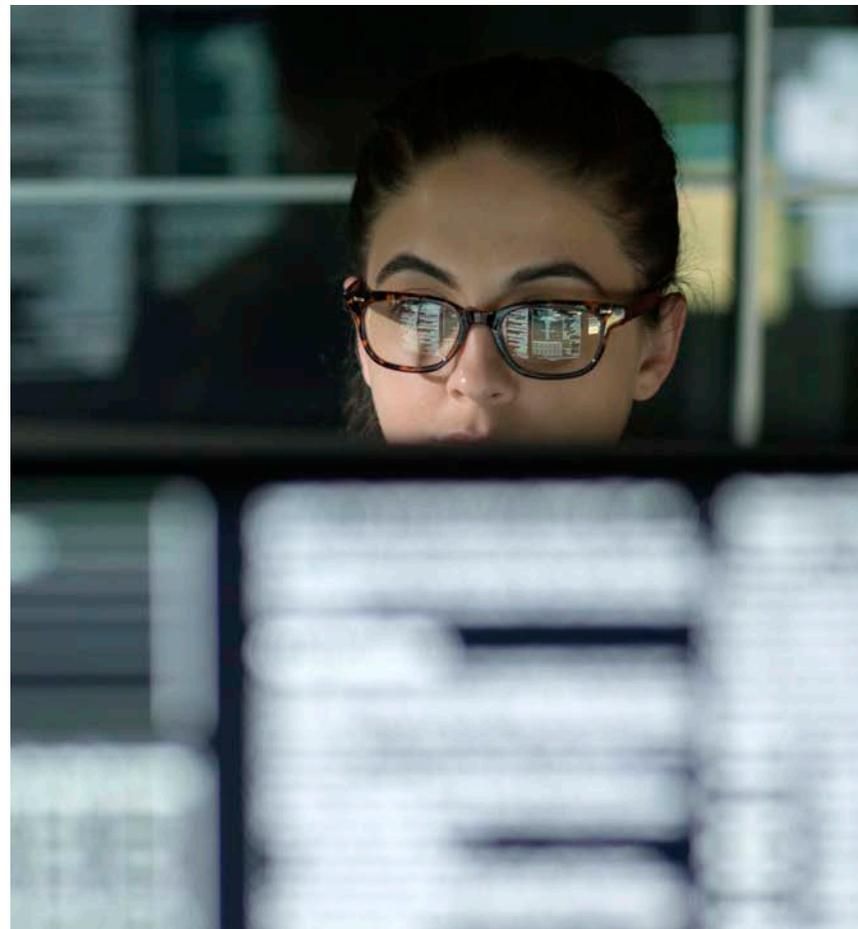
## Insight basati sui dati per ottimizzare le operazioni IT

Gli analytics possono comportare enormi risparmi per l'IT in termini di tempo ed efficienza. Gli analytics possono fornire insight su aspetti come le prestazioni di applicazioni e reti, analizzare il comportamento degli utenti, individuare i tempi di ritardo e fare previsioni sulle future esigenze IT.

Di conseguenza, gli amministratori possono individuare e comprendere meglio i trend all'interno degli ecosistemi IT, così da prendere le misure necessarie per risolvere i problemi, assicurando che i dipendenti abbiano una connessione rapida e continua.

Gli analytics possono aiutare ad affrontare i problemi aziendali e IT in vari modi, ecco alcuni esempi:

- Previsione della domanda di servizi IT
- Identificazione di potenziali interruzioni nelle operazioni o nelle catene di approvvigionamento
- Concentrazione dei servizi di assistenza dove più necessario
- Determinazione dell'efficacia di soluzioni uniche





“

Le aziende che possono automatizzare le attività di routine riescono a dedicare più tempo ad altre attività di maggiore valore.”

---

McKinsey

## Insight basati sui dati per migliorare la sicurezza

**Il monitoraggio del punteggio di rischio è un altro esempio di come gli analytics possono influire sull'efficienza di un'organizzazione. Assegnando un punteggio in base a fattori di rischio come identità, posizione, comportamento e credenziali dell'utente, il monitoraggio del punteggio di rischio consente di autorizzare gli utenti con un punteggio di rischio basso. Di contro, è possibile contrassegnare, monitorare o perfino negare l'accesso agli utenti o al traffico con un punteggio di rischio elevato fino a quando non sia possibile concedere un'autorizzazione appropriata.**

I vantaggi che ne derivano sono duplici. Il primo è abbastanza chiaro: è possibile garantire l'accesso ai file e ai dati necessari agli utenti a basso rischio. Il secondo è che, se aggregati, questi analytics evidenziano anomalie o schemi di comportamenti insoliti, semplificando l'individuazione di potenziali minacce e l'utilizzo del machine learning per prevedere i rischi futuri.

Fonte: <sup>1</sup><https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html>

+25%

Secondo uno studio, le soluzioni con analytics avanzati hanno riportato un aumento del 25% della produttività.<sup>1</sup>

## Insight basati sui dati per aumentare la produttività

Anche se alcune organizzazioni temono che i lavoratori remoti siano meno efficienti, molti studi indicano il contrario. Una ricerca condotta dal Center for Economics and Business Research (CEBR) suggerisce che i dipendenti che lavorano in remoto di fatto si distraggono per una quantità di tempo minore al giorno (27 minuti) rispetto alle loro controparti in ufficio (che accumulano 37 minuti di distrazione al giorno).<sup>1</sup>

Fonte: <sup>1</sup> [https://www.citrix.com/content/dam/citrix/en\\_us/documents/white-paper/economic-impacts-flexible-working-us-2019.pdf](https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/economic-impacts-flexible-working-us-2019.pdf)



# Il futuro sarà sempre pieno di incognite. Preparatevi con Citrix Workspace.

La vostra organizzazione ha bisogno di una soluzione IT affidabile, indipendentemente da ciò che sta accadendo nel mondo che ci circonda.



Noi di Citrix sappiamo per esperienza che una forza lavoro remota può essere produttiva. Facciamo affidamento sulla nostra tecnologia per mantenere produttivi i nostri dipendenti e serviamo i clienti per garantire la produttività anche dei loro dipendenti. Se i vostri dipendenti lavorano in ufficio, da remoto o tramite una modalità ibrida, in ogni caso Citrix Workspace può aiutarvi a semplificare la fornitura dell'IT, a proteggere il vostro ecosistema IT e ad utilizzare analytics basati sui dati per offrire continuamente esperienze eccezionali ai dipendenti.

Per maggiori informazioni, visitate [Citrix.it/workspace](https://Citrix.it/workspace).

