

Rispondere alle sfide del lavoro ibrido con la tecnologia

Come garantire il benessere e la produttività dei dipendenti nel nuovo scenario lavorativo?



È l'inizio di una nuova fase nel mondo del lavoro: l'ibrido.



A luglio 2021, il 92% dei responsabili IT ha dichiarato che la propria azienda aveva già adottato o era in procinto di adottare un modello ibrido.¹ Ciò significa un numero sempre crescente di dipendenti che lavorano secondo una combinazione di modalità, tra ufficio, casa e sedi di co-working. E sebbene il 57% si sia detto entusiasta delle prospettive,¹ e il 44% ritenga che si tratti di un passo nella giusta direzione,¹ il 78% ha anche previsto che questo cambiamento diventerà un vero e proprio peso per l'IT.²

Molte organizzazioni stanno utilizzando l'esperienza acquisita in due anni di sconvolgimenti a livello globale per definire i loro piani a lungo termine. E si sono resi conto di una cosa: i loro team IT non possono fare tutto da soli. A volte occorrono servizi supplementari per coprire le basi per le quali non dispongono delle risorse necessarie.

Le aziende stanno imparando che l'outsourcing a una piattaforma basata su cloud e supportata da servizi IT esperti crea un ecosistema digitale in cui i dipendenti possono muoversi senza limiti da un ambiente all'altro.

68%

La percentuale di lavoratori americani secondo cui l'ibrido casa-ufficio è il modello di lavoro perfetto³

70%

La percentuale di aziende che prevede per il futuro un mix di lavoro in sede e da remoto⁴

63%

La percentuale di aziende a forte crescita che ha adottato modelli di lavoro ibridi³

Si sta acquisendo consapevolezza della libertà che deriva da un "bioma tecnologico" in cui l'IT può gestire i dispositivi con tutta l'efficienza di strumenti quali la telemetria globale, l'apprendimento automatico e l'analisi predittiva. Attraverso l'automatizzazione e l'esternalizzazione delle attività più dispendiose in termini di tempo, si può aumentare la produttività dei dipendenti e prevenire il sovraccarico del proprio personale IT.



Servizi per esigenze specifiche



A contendersi l'attenzione del reparto IT, già sotto pressione, è una moltitudine di attività mission-critical. Un fornitore di servizi esperto e reattivo potrebbe dare al vostro IT un po' di sollievo nella gestione dei pressanti requisiti degli ambienti di lavoro ibridi.

Ma come decidere se un approccio basato sui servizi è adatto alla propria azienda, e quali sono le capacità essenziali che deve presentare il fornitore? Partite con l'esaminare gli elementi specifici di una configurazione di lavoro ibrida. A prescindere dai loro vantaggi, i contratti di servizio flessibili aggiungono complessità e rischi sia per l'azienda che per i singoli dipendenti.

Dopo aver chiarito meglio le vostre necessità e i punti critici, sarete più preparati a scegliere il partner giusto per la crescita della vostra azienda.

3,5%

La percentuale di fornitori di servizi intervistati da Forrester che prevede una crescita della richiesta di servizi basati sui risultati⁵

85%

La percentuale di aziende che ha accelerato, gradualmente o in modo deciso, l'implementazione di tecnologie per la collaborazione a distanza⁶

Solo il 38%

dei datori di lavoro ha aggiornato la propria tecnologia video per consentire una collaborazione più ibrida⁷



Dispositivi progettati per le esigenze di oggi



Il numero di dipendenti che accede da remoto alle risorse aziendali (reti, applicazioni, dati, supporto...), spesso da dispositivi personali come smartphone, laptop, tablet e stampanti, è in continua crescita. Ciò rappresenta una sfida multiforme per i team IT.

Per garantire la produttività dei dipendenti può essere necessario configurare nuovi dispositivi per lo smart working, gestire un maggior numero di richieste di assistenza IT e mettere in campo ulteriori strumenti di collaborazione da remoto. Oltre a queste e altre esigenze, sui responsabili IT grava anche la gestione dei costi.

Per ridurre la pressione sul vostro team IT, è possibile affidarsi a servizi di supporto esterni, evitando così di dover ricorrere a nuove assunzioni a tempo pieno, soprattutto in un periodo in cui queste risorse scarseggiano.

Quando dovrete scegliere il fornitore giusto per garantire l'efficienza delle vostre modalità di lavoro ibride, valutate i tipi di assistenza forniti per ogni fase del ciclo di vita dei dispositivi. Non tutti i fornitori, infatti, offrono un portfolio completo di servizi in grado di alleggerire veramente e con efficacia i compiti del vostro team IT.

Ecco alcune domande importanti per selezionare il vostro potenziale partner di servizi.

Potete aiutarmi nella valutazione dell'attuale ambiente IT e consigliarmi il giusto approccio per passare a un approccio moderno di gestione degli endpoint?

Fornite modelli di prezzo scalabili e flessibili per l'acquisto as-a-service? Dispositivi e applicazioni sono configurati in fabbrica prima della spedizione?

Siete in grado di eseguire il deployment rapido di dispositivi e servizi, con un'interruzione minima della produttività dei dipendenti, indipendentemente da dove lavorano?

Siete in grado di soddisfare esigenze diverse in più aree geografiche e di adattare i servizi ai requisiti locali?

Quali strumenti offrite per ottimizzare le prestazioni di sistema e gestire l'infrastruttura dei dispositivi?

Come gestite le esigenze di fine vita, il recupero dei dispositivi, la disinstallazione, la cancellazione sicura dei dati e il riciclo delle apparecchiature?

85%

La percentuale di CIO secondo cui la produttività dei dipendenti tra casa e ufficio rimane invariata²



Una gestione dei dispositivi sempre al passo con le esigenze degli utenti



Il passaggio al cloud offre modalità più efficaci per supportare i dipendenti che lavorano da remoto o in modo ibrido.

Il cloud, infatti, consente di accedere a una gamma più ampia di tecnologie e di collaborare in modo più soddisfacente. Tuttavia, la gestione di ulteriori dispositivi può mettere a dura prova un team IT già alle prese con problemi di tempo e di budget.

Il ricorso a un fornitore di servizi esterno può consentire di stare al passo con le esigenze del lavoro ibrido, automatizzando le attività di gestione dei dispositivi e utilizzando piattaforme di analisi per risolvere i problemi prima che si ripercuotano sui dipendenti.

Queste tipologie di servizi cloud-based sono efficaci per il business quando un fornitore può dimostrare che il suo supporto riduce i costi e la complessità, eliminando la necessità di ricorrere ad aumenti del personale interno.

88%

La percentuale di responsabili IT secondo cui è essenziale per i dipendenti lavorare in modo efficace ed efficiente da remoto²

Ecco alcune considerazioni da tenere presente.

In che misura il fornitore di servizi monitorerà lo stato di salute e il livello di sicurezza dei miei dispositivi?

Riceverò informazioni utili sulle prestazioni dei notebook, delle workstation, delle stampanti, dei dispositivi mobili e persino delle soluzioni di videoconferenza presenti nel mio ambiente operativo multi-sistema?

Sarò in grado di monitorare e gestire quali dispositivi sono connessi alla mia rete e quali applicazioni sono installate?

Il fornitore può aiutarmi a trasformare flussi di lavoro basati su documenti cartacei, integrandoli con il cloud e il mondo digitale?

Quanto rapidamente riceverò dettagli completi sulle cause degli errori o degli arresti anomali del sistema?

Il fornitore dispone di capacità di analisi predittiva per identificare i problemi prima che impattino sulla produttività?

In che modo il fornitore rileva eventuali non conformità rispetto alle politiche di sicurezza aziendali?

Una sicurezza che protegge persone e dispositivi



62% L'aumento degli attacchi ransomware nel 2021⁸

54% La percentuale di professionisti IT secondo cui gli smart worker rappresentano un rischio maggiore per la sicurezza rispetto a chi lavora in sede⁹

75% La percentuale di responsabili IT che riferiscono un aumento della spesa aziendale per gli strumenti di sicurezza negli ultimi 12 mesi²

La protezione di dispositivi e dati da attacchi informatici sempre più sofisticati, ma anche da violazioni per errori accidentali, è un obiettivo costante per i professionisti dell'IT. Il passaggio al lavoro ibrido, ovviamente, ha amplificato questa problematica. Nell'ultimo mese del 2021, organizzazioni di tutto il mondo hanno subito più di 722 milioni di attacchi in 30 giorni.¹⁰

I rischi potenziali emergono ogni volta che qualcuno si collega alla rete aziendale utilizzando un dispositivo personale, accede a informazioni sensibili tramite connessioni Wi-Fi domestiche o pubbliche, installa applicazioni non autorizzate o viaggia con un dispositivo aziendale.

L'approccio BYOP (bring-your-own-printer) comporta ulteriori rischi, che rientrano in quell'area denominata "shadow IT". Le stampanti personali dei dipendenti, infatti, non sono di competenza dell'IT aziendale, pur non disponendo generalmente delle configurazioni di sicurezza necessarie.

Come riporta il Security Magazine: "L'uso di software non autorizzati e di shadow IT può mettere a rischio la sicurezza informatica dell'intera azienda".¹¹

È inevitabile che qualcosa sfugga, a meno che non si metta in campo una qualche sentinella sempre attiva e vigile su strumenti e servizi in grado di coprire le spalle all'IT, riducendo rischi e stress.

Per definirsi efficace, un approccio alla sicurezza deve proteggere l'organizzazione senza aggiungere complessità ai dipendenti o al personale IT. Occorre tenere presente, infatti, che le esigenze in termini di sicurezza vanno combinate con una miriade di altre priorità portate avanti dal reparto IT.

Ecco alcune importanti aree da analizzare.

Il fornitore di servizi di sicurezza in questione è in grado di aggiungere rapidamente una difesa a più livelli al mio ambiente di lavoro remoto, senza aumentare il carico di lavoro dell'IT?

Il fornitore offre una protezione integrata per i dispositivi endpoint, le applicazioni basate su cloud, l'hardware di rete e i punti di contatto web?

Il fornitore dispone di un gruppo di esperti di sicurezza? È possibile quantificare il supporto continuo che riceverà il mio reparto IT?

Posso contare su questi servizi per identificare e risolvere in modo proattivo i potenziali rischi per la sicurezza prima che causino danni effettivi?

Qual è l'approccio del fornitore per mantenere una sicurezza non invasiva, in modo che i dipendenti possano concentrarsi sul loro lavoro quotidiano?

Gli strumenti giusti per i vostri dipendenti e il vostro personale IT.

Il lavoro dell'IT è fondamentale. Ecco perché aziende di ogni dimensione stanno scoprendo i vantaggi dell'adottare servizi gestiti per PC, stampanti, smartphone, soluzioni di videoconferenza e altre tecnologie su cui fa grande affidamento una forza lavoro sempre più ibrida. Potenziando le vostre risorse IT con i servizi HP potrete rivoluzionare il modo in cui operate, aumentando efficienza e produttività per i vostri dipendenti, ovunque essi lavorino.

PIÙ LIBERTÀ PER I DIPENDENTI con soluzioni **PERSONALIZZATE** che soddisfano esigenze e stili di lavoro diversi: dispositivi versatili, esperienze coinvolgenti, supporto ergonomico e strumenti abilitati al cloud.

PIÙ SICUREZZA CONTRO LE MINACCE IN CRESCITA con soluzioni che **PROTEGGONO** il vostro personale e i vostri dati: tecnologia zero trust, isolamento e contenimento, aggiornamenti automatici e servizi gestiti.

MENO PRESSIONE SUL VOSTRO TEAM IT con soluzioni che lo rendono più produttivo in presenza di richieste e responsabilità crescenti: automazione IT, flussi di lavoro digitalizzati, gestione moderna dei dispositivi, configurazione e deployment da remoto.

PRONTI A SODDISFARE ESIGENZE IN CONTINUA EVOLUZIONE con soluzioni che rispondono agli obiettivi specifici dei vostri team IT e della vostra azienda: insights in tempo reale, soluzioni configurabili, gestione degli endpoint e del ciclo di vita.

Offrite al vostro personale IT il supporto di cui ha bisogno per rendere il lavoro ibrido meno gravoso. Per saperne di più visitate hp.com/hp-services —>

¹ Snow Software, "Study: Hybrid Work Is Here to Stay, Bringing Its Own Mix of Complexities," 29 luglio 2021, <https://www.snowsoftware.com/blog/study-hybrid-work-here-stay-bringing-its-own-mix-complexities>

² Snow Software, "2022 IT Priorities Report," dicembre 2021, https://go.snowsoftware.com/rs/377-PWR-208/images/2022_Snow_IT_Priorities_Report_12.6.21_FINAL.pdf

³ Apollo Technical, "19 Important Hybrid Working Statistics to Know Now and for the Future (2021)," 6 gennaio 2022, <https://www.apollotechnical.com/hybrid-working-statistics>

⁴ CNBC, "The latest numbers on how many workers will be returning to offices, and how often," 8 luglio 2021, <https://www.cnbc.com/2021/07/08/how-many-workers-will-be-returning-to-offices-and-how-often.html>

⁵ Forbes, "5 Ways To Support Hybrid Working In The Future Workplace," 15 marzo 2021, <https://www.forbes.com/sites/nigeldavies/2021/03/15/5-ways-to-support-hybrid-working-in-the-future-workplace/?sh=4cefa823373d>

⁶ The Enterprisers Project, "Hybrid work's next phase: 3 lessons for CIOs," 29 ottobre 2021, <https://enterpriseproject.com/article/2021/10/hybrid-work-next-phase-3-lessons>

⁷ Owl Labs, "New Hybrid Work Statistics: The 5th Annual State of Remote Work Report," 11 novembre 2021, <https://resources.owlabs.com/blog/state-of-remote-work-report-2021>

⁸ Intras Cloud Services, "5 Ways to Protect Yourself from Cyber Security Threats in 2022," 2 gennaio 2022, <https://www.intrasclooudservices.com/blog/5-ways-to-protect-yourself-from-cyber-security-threats-in-2022/>

⁹ Findstack, "The Ultimate List of Remote Work Statistics for 2022," 6 dicembre 2021, <https://findstack.com/remote-work-statistics>

¹⁰ Cybercrime Magazine, "Organizations Worldwide Experience Over 722 Million Attacks In The Last 30 Days!" 29 dicembre 2021, <https://blog.knowbe4.com/organizations-worldwide-experience-over-722-million-attacks-in-the-last-30-days>

¹¹ Security Magazine, "Top 5 cybersecurity challenges in the hybrid office," 16 giugno 2021, <https://www.securitymagazine.com/articles/95434-top-5-cybersecurity-challenges-in-the-hybrid-office>

I servizi HP sono regolati dalle condizioni generali HP previste per il servizio fornito o indicate al cliente al momento dell'acquisto. Il cliente potrebbe disporre di ulteriori diritti legali a seconda delle leggi locali vigenti; tali diritti non sono in alcun modo alterati dai termini e dalle condizioni di servizio HP o dalla garanzia limitata HP fornita con un prodotto HP.

© Copyright 2023 HP Development Company, L.P. Le informazioni qui contenute possono subire variazioni senza preavviso. Le uniche garanzie sui prodotti e sui servizi HP sono espresse nelle dichiarazioni di garanzia esplicita che accompagnano i suddetti prodotti e servizi. Nulla di quanto qui contenuto può essere interpretato come garanzia aggiuntiva. HP declina ogni responsabilità per errori tecnici o editoriali od omissioni qui contenuti.