

Virtual Desktop Infrastructure 365

La postazione di lavoro online senza compromessi

L'evoluzione del modo di lavorare dei dipendenti e dei collaboratori aziendali, ha determinato che il tema della sicurezza del lavoro da remoto, al di fuori dei perimetri aziendali, sia un argomento di alta attenzione da parte dei CIO e dei dipartimenti IT. La capacità di supportare e gestire una forza lavoro remota è essenziale per mantenere la continuità aziendale ed offrire un ambiente di lavoro protetto, affidabile e sicuro.



Protetto

Massima protezione delle identità, i dispositivi e le informazioni. Il rischio di perdita e danneggiamento dei dati dev'essere ridotto al minimo



Affidabile

Garantire la disponibilità delle risorse necessarie per essere sempre in linea ed operativi: accedere ai servizi aziendali ed ai siti web senza restrizioni



Sicuro

Garantire l'accesso protetto e controllato ai sistemi ed ai servizi aziendali e consentire l'utilizzo sicuro dei dispositivi personali a scopi lavorativi

Virtual Desktop Infrastructure 365 è la nuova soluzione di Microsys basata su tecnologia **Microsoft Azure** che ospita i desktop aziendali in remoto e consente agli utenti di accedere in mobilità al proprio ambiente di lavoro da ogni computer. Virtual Desktop Infrastructure 365 è particolarmente utile alle aziende che hanno i dipendenti che lavorano da casa, o in mobilità, poiché garantisce la disponibilità e l'accesso alla postazione di lavoro costantemente aggiornata senza il coinvolgimento del dipartimento IT.

Virtual Desktop Infrastructure 365:



Sicurezza

Utilizzo sicuro da remoto dei dati, le applicazioni ed i servizi aziendali



Ambiente di Lavoro Agile

Disporre da remoto della piattaforma di lavoro affidabile, dinamica e sempre aggiornata come se si fosse in sede



Abilita il cambiamento

Portare in azienda le politiche per usare i dispositivi personali sul lavoro con accessi privilegiati alle informazioni ed alle applicazioni aziendali

Microsys Virtual Desktop Infrastructure 365

1

La soluzione VDI basata su Azure che consente l'accesso ubiquo a tutte le applicazioni interne, a qualsiasi file server della rete interna e in generale a tutto quanto è normalmente disponibile agli utenti interni, ma senza esporre la rete e senza portare all'interno le macchine remote. In questo modo si mantiene il controllo della parte interna e si può rinunciare a controllare quella esterna, perché in realtà non ci interessa come è configurata. Utilizzando l'autenticazione integrata con Acrive Directory e abilitando MFA si ottiene un elevato livello di sicurezza unito ad una ragionevole semplicità di accesso per l'utente.

2

Garantisce la sicurezza degli accessi da parte degli amministratori di sistema, da ovunque accedano. Le credenziali amministrative non vengono mai usate da macchine personali, ma sempre e solo dalle macchine virtuali dedicate agli amministratori, e solo dopo che l'identità del sistemista è stata verificata tramite MFA. In questo modo nemmeno un keylogger (un malware che "legge" quello che l'utente digita e di conseguenza è in grado di carpire una password) potrebbe aggirare le protezioni.

3

Semplifica la gestione dell'infrastruttura IT in quanto gli aggiornamenti del software possono avvenire in modalità centralizzata.