Dell Technologies consiglia la piattaforma Intel vPro®: creata per il business

I dipendenti stanno scegliendo come lavorare

E con la giusta strategia digitale sicura, questo potrebbe essere un ottimo cosa per il tuo business: oggi e nel futuro

DELL Technologies

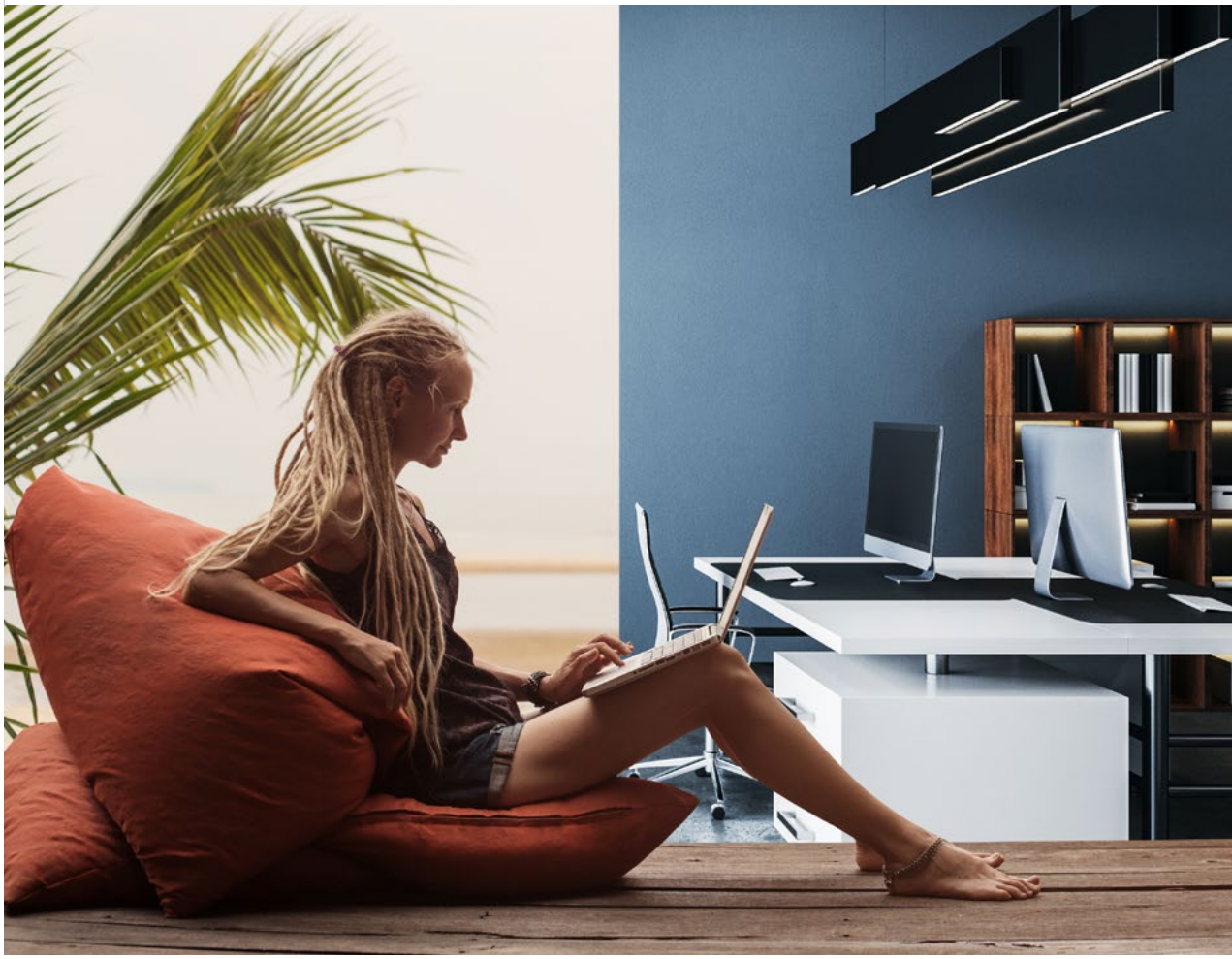
Innovation Built-In intel

Sommario

1

Il lavoro è cambiato e lo farà di nuovo

I dipendenti stanno ridefinendo l'ambiente di lavoro come mai prima d'ora e le aziende smart ne traggono vantaggio



Sommario

"La misura dell'intelligenza è la capacità di cambiare".

Questa citazione, attribuita ad Albert Einstein, è particolarmente adatta al cambiamento sismico che sta avvenendo oggi nei nostri ambienti di lavoro. In pochi non sarebbero d'accordo sul fatto che il modo in cui lavoriamo oggi è molto diverso da quello di pochi anni fa. Le organizzazioni hanno dovuto migliorare le proprie strategie tecnologiche per consentire alle persone di lavorare da qualsiasi luogo e di interagire con i clienti in nuovi modi digitali, sia che fossero entusiaste delle possibilità del cambiamento, sia che si sentissero disturbate da esso.

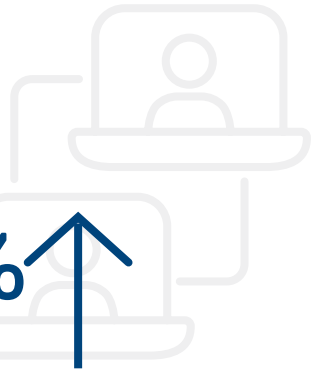
Per rimanere connessi, produttivi e sicuri in un mondo in cui molte forme di lavoro possono essere svolte da remoto, i dipendenti devono essere certi che l'ambiente digitale non ostacolerà la loro capacità di dare il meglio di sé. Una ricerca globale di Statista mostra che l'80% dei dipendenti che lavorano almeno parzialmente da remoto lo consiglierebbe a un amico. Tuttavia, come osserva lo studio, "l'atteggiamento nei confronti del telelavoro è positivo se ai dipendenti vengono forniti gli strumenti e le tecnologie adeguate per lavorare da remoto. Questi includono strumenti di collaborazione digitale e di gestione della produttività, oltre all'hardware necessario".[1]

Questi atteggiamenti stanno modificando profondamente il ruolo della funzione IT nelle organizzazioni di tutto il mondo. Oggi più che mai, il ruolo dei leader IT nell'offrire una moderna esperienza digitale ai dipendenti, fornendo un accesso sicuro a tutti gli strumenti e le risorse necessarie per i diversi ruoli, sta portando un netto vantaggio nella produttività delle aziende più lungimiranti. Una ricerca condotta nel 2021, ad esempio, ha rilevato che chi ha accesso al lavoro da remoto ha aumentato l'innovazione del 63%, l'impegno lavorativo del 75% e l'impegno organizzativo del 68%.[2]

Dare priorità all'esperienza dei dipendenti

I team IT sono consapevoli di questa crescente responsabilità. L'analisi di Gartner prevede che "entro il 2025, oltre il 50% delle organizzazioni IT utilizzerà l'esperienza digitale dei dipendenti per definire le priorità e misurare il successo delle iniziative digitali, con un aumento significativo rispetto a meno del 5% nel 2021".[3] C'è un chiaro spostamento verso la collocazione delle esigenze digitali specifiche dei dipendenti al centro della strategia digitale, con l'IT come motore per la creazione di nuove opportunità di business mentre l'ambiente di lavoro si evolve oggi e continuerà a farlo domani.

In questo documento, Dell Technologies e i nostri partner di Intel analizzano le principali sfide e opportunità che emergono dal cambiamento dell'ambiente di lavoro. Insieme, definiamo le best practice di leadership IT che garantiranno ai dipendenti di lavorare, collaborare e innovare in modo protetto e produttivo da qualsiasi luogo e, soprattutto, di accompagnare l'azienda verso i suoi obiettivi.



63%

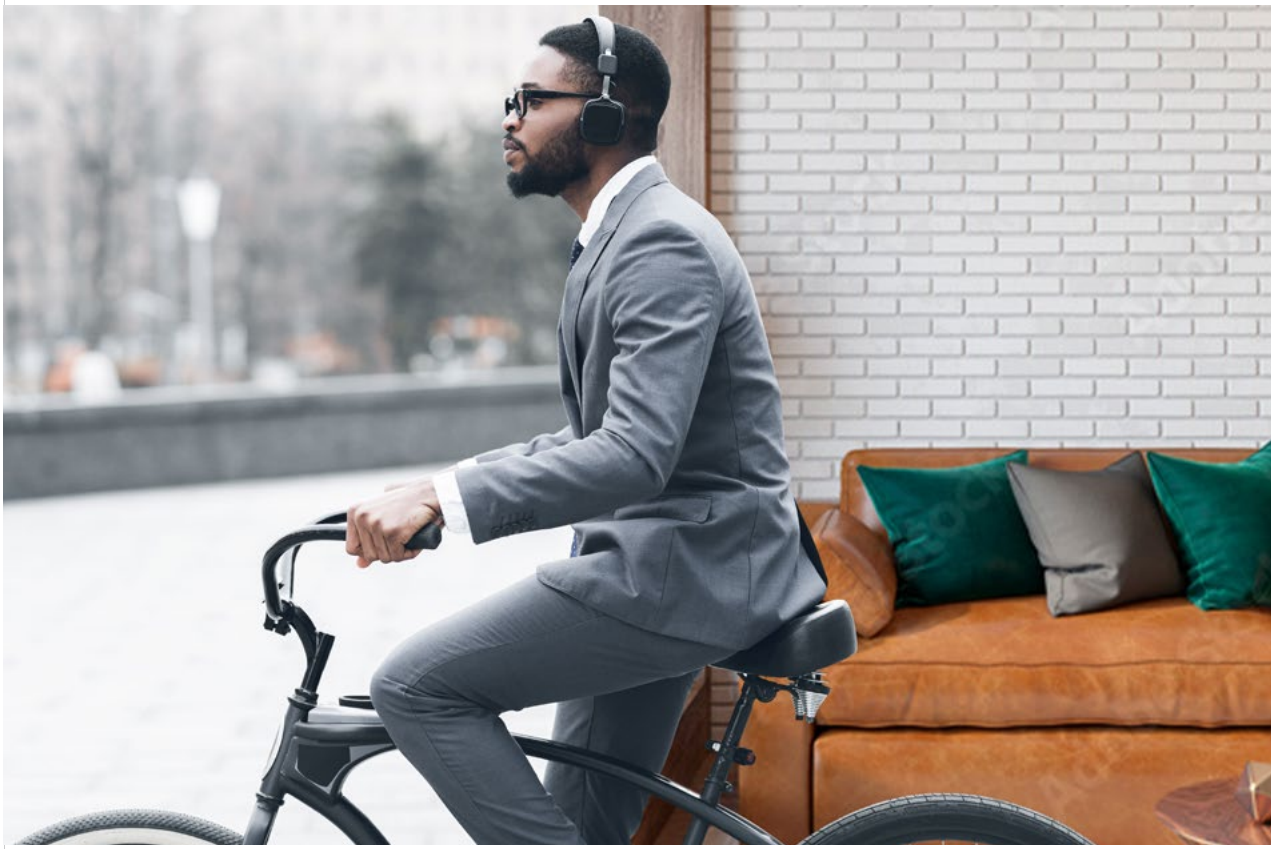
di aumento dell'innovazione grazie all'accesso al lavoro da remoto

Sommario

2

Lezioni passate, nuove opportunità

Cosa ci dicono i cambiamenti tecnologici storici sul futuro e come trarne il massimo vantaggio per l'azienda



Sommario

Affrontiamo un tema impegnativo e a volte divisivo. Per molti leader aziendali può sembrare contro intuitivo che le esigenze tecnologiche di lavoro da remoto dei dipendenti possano dettare il modo in cui un'organizzazione deve operare e innovare. Ma il cambiamento dell'ambiente di lavoro sta avvenendo ugualmente.

In occasione della pubblicazione del report Global Talent Trends 2022 di LinkedIn, Jennifer Shappley, responsabile globale dell'acquisizione di talenti, ha dichiarato: "Il contratto tra dipendenti e datori di lavoro viene riscritto. Ciò che per i dipendenti era accettabile, adesso non lo è più. Quando non sentono attenzione e sostegno da parte dei loro datori di lavoro, se ne vanno". [4]

Adattarsi ai cambiamenti

In questo clima, i dirigenti devono prendere una decisione fondamentale: mantenere la strategia attuale o adattarsi alle forze del cambiamento dell'ambiente di lavoro. Nella competizione per i talenti qualificati, le organizzazioni in rapida evoluzione stanno scegliendo di adattarsi: Ladders, sito specializzato in carriere, prevede che il 25% degli ambienti di lavoro ad alta retribuzione sarà disponibile da remoto entro la fine del 2022.[5]

Per coloro che ancora sono titubanti nel supportare le funzionalità di lavoro da remoto a lungo termine, in particolare per il fatto che esse confondono la linea di demarcazione tra vita personale/da consumatore e vita lavorativa/dipendente, può essere d'aiuto considerare altri momenti del passato recente in cui le tecnologie per il consumo e per l'ambiente di lavoro hanno subito una convergenza, creando vaste opportunità di business nel processo...

1. La consumerizzazione dell'IT: nel 2005, la migrazione nell'ambiente di lavoro di software e hardware progettati per uso personale è stata definita da Gartner come "la tendenza più significativa che interesserà l'IT nei prossimi 10 anni". Al giorno d'oggi è difficile immaginare un'azienda che operi senza tecnologie mobili, banda larga accessibile e la possibilità di utilizzare i dispositivi personali in un contesto lavorativo.

2. L'Internet of Things (IoT): la creazione di una rete di oggetti fisici, integrati con software e sensori e dotati della capacità di scambiare dati con altri dispositivi e sistemi, ha aperto un nuovo mondo di possibilità per i consumatori, come la gestione dell'energia domestica. Allo stesso tempo, ha offerto grandi opportunità alle aziende, come la manutenzione predittiva per migliorare l'efficienza delle fabbriche.

3. Applicazioni mobile e servizi cloud: la prima applicazione che molti hanno conosciuto è stato il gioco "Snake" sul Nokia 6110. Tuttavia, le applicazioni si sono diffuse realmente con il lancio dell'App Store di Apple nel luglio 2008. Oggi le applicazioni mobile e i servizi cloud che le supportano sono la linfa vitale della produttività quotidiana del personale delle aziende di tutto il mondo.

4. Gamification: coniata per la prima volta nel 2002 dal programmatore informatico di origine britannica Nick Pelling, con il termine "gamification" si intende l'utilizzo delle meccaniche dei giochi per aumentare l'impegno, la felicità e la fedeltà del pubblico. Oggi è una parte fondamentale dell'impegno aziendale nei confronti di dipendenti e clienti, dalla formazione al marketing.

Sommario

5. Intelligenza artificiale e apprendimento automatico: ora sono alla base di un gran numero di interazioni online e tramite app mobile, l'AI e la ML hanno una capacità apparentemente illimitata di intrattenere e coinvolgere, trasformando allo stesso tempo quasi tutti i settori e le funzioni organizzative, rendendo la vita più facile, più efficiente e potenzialmente più significativa, sia all'interno che all'esterno dell'ambiento di lavoro.

6. 5G: più i dispositivi mobili sono diventati parte integrante della nostra vita, più le reti wireless si sono evolute in termini di copertura e velocità, creando nuove opportunità per le aziende. Con l'introduzione del 5G, la connettività internet veloce e sempre attiva sta fornendo l'infrastruttura per le tecnologie su cui le aziende fanno affidamento e per quelle che devono ancora creare.

Così, come in passato l'intersezione tra tecnologia consumer e business ha creato nuove opportunità per le aziende, oggi le mutevoli preferenze lavorative e le esigenze digitali dei dipendenti possono creare nuove possibilità per le aziende, consentendo loro di sbloccare nuovo valore, rimanere competitive e superare le interruzioni.

Superare le sfide

Ma per trarre il massimo vantaggio da queste opportunità, le aziende devono superare alcune sfide fondamentali, prima fra tutte quella di affrontare i nuovi rischi legati alla sicurezza informatica. Poiché la forza lavoro, le app e i dati sono sempre più distribuiti tra sedi centrali e remote e i dipendenti utilizzano sia i dispositivi in dotazione al lavoro che quelli personali, le minacce alla sicurezza dei dati sono in aumento.

Di conseguenza, i team IT hanno sempre più difficoltà a mantenere un controllo sicuro dei loro ambienti e a farli funzionare in modo ottimale per soddisfare le esigenze aziendali. In una recente survey condotta da Vanson Bourne tra i responsabili delle decisioni IT, il 50% ha espresso la preoccupazione di mantenere la propria organizzazione al sicuro dalle crescenti minacce alla sicurezza informatica, mentre il 49% è preoccupato per la propria capacità di fornire un supporto IT proattivo e da remoto a una forza lavoro sempre più distribuita.[6]

È quindi chiaro che le organizzazioni che trarranno i maggiori vantaggi competitivi da questa nuova realtà lavorativa saranno quelle che costruiranno una cyber-resilienza orientata al futuro, che offriranno ai dipendenti un'esperienza migliorata, moderna e sicura per sostenere la produttività e che affronteranno le considerazioni culturali per garantire che tutti considerino la sicurezza come parte del loro ruolo, oggi e in futuro.

Il 25%

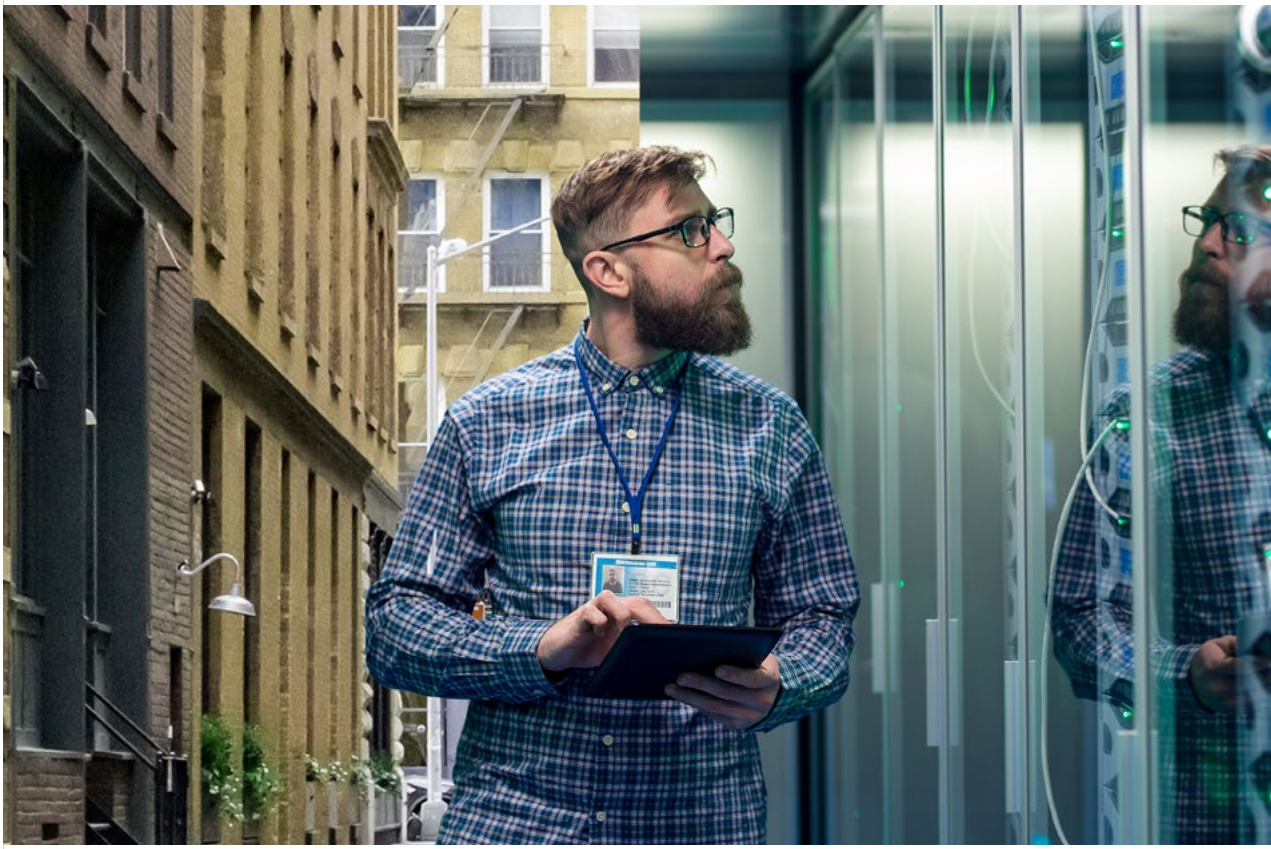
dei posti di lavoro ad alta retribuzione sarà disponibile da remoto entro la fine del 2022

Sommario

3

Un passo sicuro verso il futuro

Una ricerca dimostra che per massimizzare le opportunità di business derivanti dal lavoro ibrido è necessario concentrarsi sulla cyber-resilienza



Sommario

Di tanto in tanto tutti al lavoro hanno bisogno dell'aiuto del team IT, ma a chi si rivolge il team IT in caso di necessità? Nel tentativo di offrire esperienze digitali migliorate ovunque i dipendenti lavorino, le funzioni IT sono perfettamente consapevoli di aver bisogno di supporto.

Nello studio di Vanson Bourne, quando ai leader IT è stato chiesto in quale area avessero bisogno di assistenza per passare a un ambiente di lavoro ibrido, la risposta principale è stata "mantenere la sicurezza dei dipendenti da remoto" (48%), prima di fattori quali "migliorare la produttività" (45%) e "migliorare l'efficienza" (40%). Solo il 5% dei leader ha dichiarato di non aver bisogno di aiuto.[7]

Non c'è da stupirsi che le mutevoli esigenze di una forza lavoro sempre più distribuita abbiano creato un problema di sicurezza per i leader IT delle organizzazioni di tutto il mondo. A causa dell'evoluzione dell'ambiente di lavoro, la sicurezza degli endpoint è diventata sempre più complessa, con un perimetro di rischio esteso, applicazioni e dati forniti da una moltitudine di data center tradizionali e cloud e un rapido aumento dei dispositivi edge che devono essere protetti dalla proliferazione delle minacce informatiche.

Una visione diversa della sicurezza

Come i titoli dei giornali di tutto il mondo hanno ripetutamente evidenziato negli ultimi anni, le tattiche di attacco informatico come il ransomware sono sempre più efficaci, in tutti i settori, e hanno gravi ripercussioni sia sui bilanci che sulla reputazione delle aziende.

Infatti, nel Global Security Insights Report 2021 di VMware, il 78% dei professionisti della sicurezza intervistati ha confermato che gli attacchi sono aumentati come conseguenza del lavoro da casa dei dipendenti. E il 61% ha riconosciuto la necessità di considerare la sicurezza in modo diverso a causa dell'ampliamento della superficie delle minacce.[8] The State of Ransomware 2022 Report ha rilevato che tali attacchi avranno un impatto sul 66% delle organizzazioni nel 2021, rispetto al 37% del 2020.[9]

Migliorare la cyber-resilienza in tutto il panorama lavorativo ibrido è quindi ora un imperativo mission-critical. L'ultima ricerca di ESG del 2022 mostra una correlazione diretta tra gli investimenti nella cyber-resilienza, lo sviluppo di una maggiore efficienza dei costi e un ambiente migliore e più positivo per la produttività e l'innovazione.[10] Nello studio, i responsabili delle decisioni IT sono stati intervistati e segmentati in base al grado di maturità della cyber-resilienza nelle loro organizzazioni. Sono state poste loro quattro domande chiave:

- **Come descriveresti il livello del personale nel tuo team di sicurezza informatica?**
- **Come descriveresti il livello delle competenze nel tuo team di sicurezza informatica?**
- **Come definiresti l'investimento della tua organizzazione in prodotti e servizi per proteggere sistemi, applicazioni e dati?**
- **L'organizzazione controlla o verifica la sicurezza dei suoi partner/vendor IT?**

Solo il 5%

dei leader IT afferma di non aver bisogno di aiuto per passare a un ambiente di lavoro ibrido

Sommario

ESG ha classificato solo il 10% delle aziende "preparate" con il livello più elevato di maturità della cyber-resilienza. Queste aziende sono definite come "con un livello ottimale di investimenti in tecnologie di sicurezza, livello del personale e rigorosa ispezione dei rischi di terze parti". Il 26% successivo è stato classificato come "vulnerabile" e il restante 64% come "esposto".

Sono state identificate diverse differenze chiave tra le organizzazioni preparate e quelle con livelli inferiori di maturità nella cyber-resilienza, in particolare per quanto riguarda il valore aziendale derivante dall'utilizzo della sicurezza dei dispositivi degli utenti finali nella forza lavoro ibrida.

Ad esempio, le organizzazioni preparate hanno 2,5 volte più probabilità di garantire un uptime del 99,99% o superiore per le loro applicazioni business-critical, il che equivale a un vantaggio stimato di 33,3 milioni di dollari in termini di costi di downtime. Sono anche molto più agili quando si tratta di rilevare e rispondere agli incidenti, con un tempo medio di rilevamento del 20% più veloce e un tempo medio di ripristino del 35% più veloce. In media, queste aziende sono state in grado di ridurre l'ingombro dei dispositivi non protetti del 33%.[11]

Ritorno sul capitale investito

Dal momento che le organizzazioni inseguono un nuovo futuro lavorativo ibrido, stare al passo con il 10% delle aziende più preparate richiederà, ovviamente, investimenti in competenze, tecnologie di resilienza e un rigoroso controllo dei rischi di terze parti. Tuttavia, la ricerca mostra chiaramente che questa componente dei costi comporta un significativo ritorno sugli investimenti.

E se ora analizziamo i benefici che la resilienza può apportare all'impegno e alla produttività dei dipendenti, questo ritorno potrebbe portare un'organizzazione verso aree di opportunità che vanno ben oltre quelle attualmente accessibili ai suoi concorrenti meno maturi e più vulnerabili.

Vantaggio di 33,3 milioni di dollari

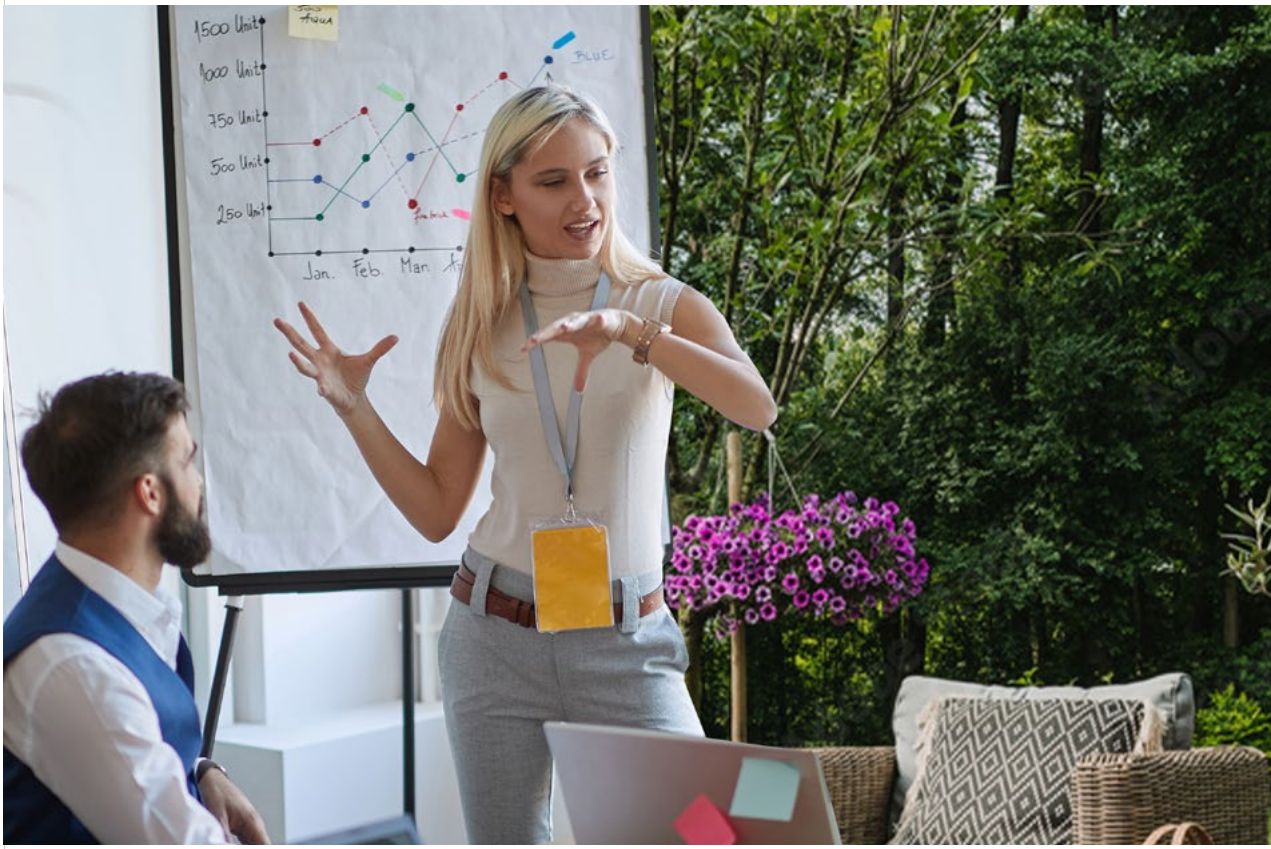
le organizzazioni preparate hanno una probabilità 2,5 volte maggiore di erogare un uptime del 99,99% o superiore, il che equivale a un vantaggio stimato di 33,3 milioni di dollari in termini di costi di downtime.

Sommario

4

Ottimizzazione della produttività dei dipendenti

Le aziende che offrono esperienze digitali sicure e senza interruzioni ai dipendenti di tutto il mondo si dimostrano più produttive rispetto a quelle che non lo fanno



Sommario

Veniamo al dunque: se non ci fossero vantaggi aziendali nel mantenere e migliorare le pratiche di lavoro ibride, la maggior parte delle organizzazioni probabilmente non perseguirebbe questa trasformazione, in un mondo senza interruzioni.

Tuttavia, in una survey globale condotta da PwC su dirigenti e leader focalizzati sulle risorse umane, pubblicata alla fine del 2021, il 57% ha dichiarato che il lavoro da remoto e ibrido ha portato la propria organizzazione a ottenere risultati migliori rispetto agli obiettivi di produttività e performance della forza lavoro negli ultimi 12 mesi, mentre solo il 4% ha dichiarato che la propria azienda ha ottenuto risultati significativamente peggiori in quel periodo.[12]

Vantaggi per l'azienda

La produttività aziendale, e quindi i profitti e la crescita, è una delle motivazioni chiave che spingono a promuovere il lavoro ibrido. È quindi naturale che consentire alle persone di lavorare in modo sicuro e conforme, dove e come preferiscono, sui dispositivi che preferiscono, sia uno degli obiettivi principali delle organizzazioni che stanno abbracciando il futuro del lavoro ibrido.

Perché quando i lavoratori hanno la libertà di lavorare senza attriti dove e come vogliono, possono rimanere concentrati sugli obiettivi organizzativi principali, rafforzando il loro impegno verso l'azienda.

Ad esempio, la ricerca di ESG del 2022 sulla cyber-resilienza e le prestazioni degli utenti finali mostra che i dipendenti delle organizzazioni "preparate" assegnano ai loro team IT un punteggio di soddisfazione cinque volte superiore rispetto a quelli delle organizzazioni "esposte".[13]

Per i leader aziendali, questo si sta traducendo in un vantaggio per l'azienda: queste stesse organizzazioni hanno una probabilità 7,7 volte superiore rispetto a quelle esposte di immettere sul mercato nuove offerte prima della concorrenza e prevedono che i loro ricavi cresceranno a un tasso doppio rispetto ai loro colleghi.[14]

Questi dati si basano su una ricerca condotta da ESG a metà del 2021, che ha analizzato la correlazione tra l'adozione di una moderna tecnologia dei dispositivi e il successo e la resilienza dell'azienda. Lo studio ha rilevato che le organizzazioni che possono essere classificate come "Digital Workplace Accelerators" registrano in media il 18% in meno di eventi critici legati alla compromissione dei dispositivi.

Le stesse organizzazioni proattive hanno anche 2,1 volte più probabilità di superare gli obiettivi di soddisfazione del cliente rispetto alle loro controparti più reattive e, in media, il 40% in più del loro fatturato annuale deriva da offerte innovative e di nuova concezione.[15]

Sommario

Luoghi pubblici, dati privati

Ma se la creazione di ambienti digitali sicuri e privi di attrito per i lavoratori da remoto e ibridi comporta evidenti vantaggi aziendali, come la mettiamo quando questi lavoratori non riescono a trovare uno spazio completamente privato in cui operare?

Molti dipendenti sono giustamente preoccupati, e a volte addirittura distratti, di lavorare con informazioni sensibili che potrebbero essere viste da altri negli spazi pubblici. Si tratta di una preoccupazione assolutamente legittima, dal momento che uno studio del 2022 ha rilevato che il 62% dei pendolari nel Regno Unito ammette di aver sbirciato gli schermi degli smartphone dei compagni di viaggio.[16]

Quando lavorare in uno spazio completamente privato non è un'opzione possibile, le aziende devono comunque garantire che i loro dipendenti possano essere fiduciosi e produttivi in modo sicuro e senza interruzioni, grazie a dispositivi progettati per garantire una privacy intelligente.

Gli attuali leader IT dovrebbero quindi richiedere ai loro partner tecnologici affidabili dispositivi moderni che eroghino ai dipendenti un'esperienza produttiva intuitiva, aiutandoli al contempo a proteggere le risorse digitali e a mantenere sempre riservati i dati sensibili.

Tecnologie avanzate per la privacy

Per esempio, questo significa insistere su una suite completa di funzioni intelligenti per la privacy, come il "rilevamento di chi guarda", che può notificare all'utente la presenza di un osservatore nei paraggi e texturizzare istantaneamente il display o attivare la modalità schermo sicuro.

I PC più avanzati di oggi sono anche in grado di oscurare lo schermo nel momento in cui l'utente distoglie lo sguardo, per dare al dipendente la certezza che i suoi dati rimangano protetti anche se all'improvviso deve rivolgere la sua attenzione altrove.

I vantaggi in termini di produttività e di profitto che derivano dalla possibilità di lavorare da remoto e in modalità ibrida in modo sicuro e ottimale sono ormai ben documentati e l'evidenza continua a crescere. Con la giusta strategia digitale e i giusti dispositivi, le organizzazioni di tutti i settori possono offrire ai dipendenti esperienze lavorative sicure e senza interruzioni che da oggi aumenteranno il loro vantaggio in questo campo. Ma, come andremo a vedere, per far sì che i vantaggi durino nel tempo c'è un elemento culturale fondamentale da considerare...

40%↑

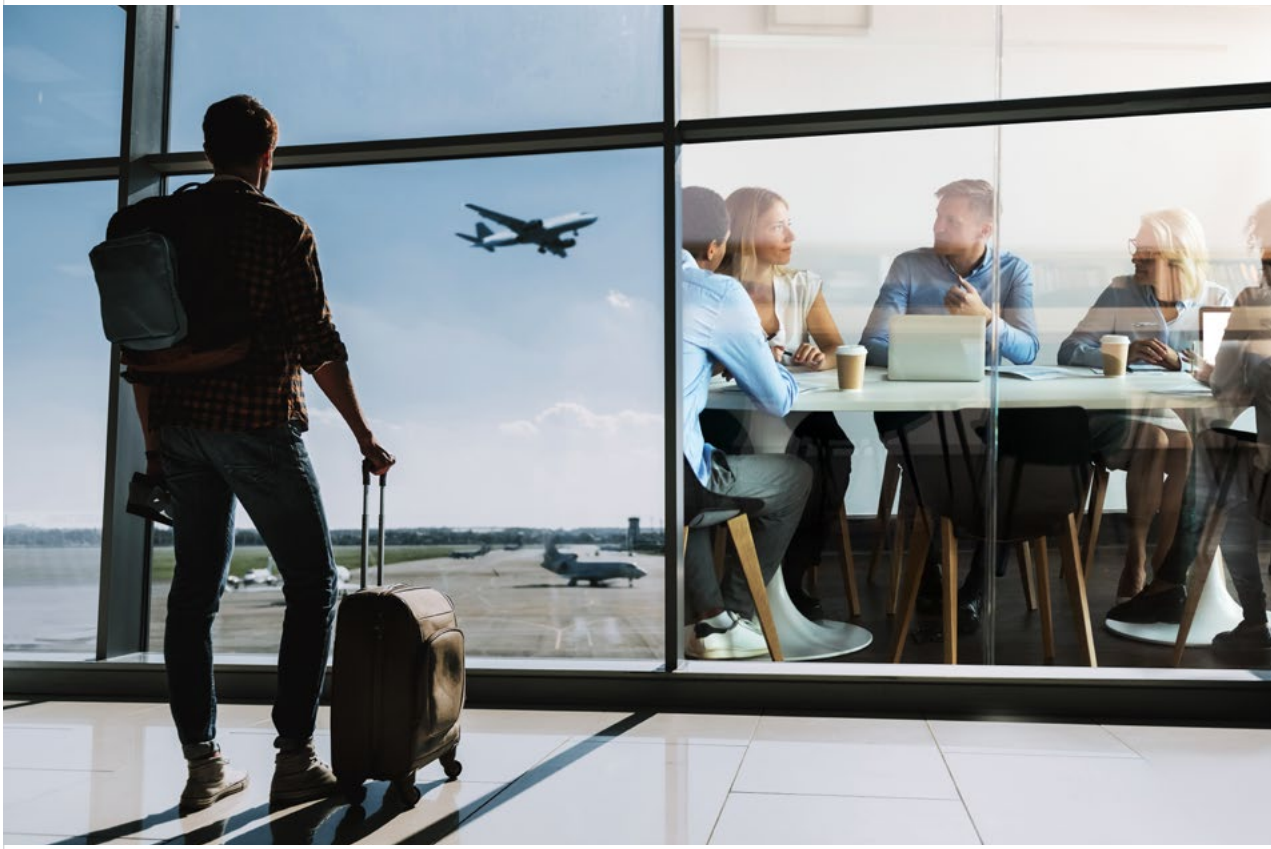
in più di ricavi derivanti da offerte innovative e di nuova concezione presso le organizzazioni considerate "Digital Workplace Accelerators"

Sommario

5

Perché la sicurezza è il business di ogni persona

Se le aziende vogliono ottenere vantaggi duraturi dal lavoro ibrido, la sicurezza non può essere delegata al team IT



Sommario

Come i tre porcellini della classica favola per bambini, i dipendenti che lavorano da remoto e in modo ibrido devono affrontare sia i tentativi coercitivi ("let me come in") che quelli violenti ("I'll blow your house down") di violare la loro sicurezza. Sfortunatamente, i cybercriminali di oggi hanno modi molto più sottili e sofisticati per entrare rispetto a quelli utilizzati dal lupo cattivo della favola.

Prendiamo ad esempio il recente attacco di phishing "browser-in-the-browser", o "BitB", che simula in modo convincente finestre di secure sign-on (SSO) per rubare le credenziali di accesso, ad esempio per gli account Google e Microsoft. È l'ultimo esempio della rapida evoluzione del mondo della "social engineering" malevola, che è stata riassunta in modo chiaro in un recente podcast del MIT Technology Review da John Scimone, Presidente e Chief Security Officer di Dell Technologies:

"La social engineering, in particolare, continua a essere una delle principali preoccupazioni", ha affermato. "Per coloro che non hanno familiarità con la social engineering, si tratta essenzialmente del tentativo da parte dei criminali di indurre i dipendenti a consegnare informazioni o ad aprire le porte per consentire ai criminali di entrare nel loro sistema, ad esempio attraverso le e-mail di phishing, che continuiamo a vedere come uno dei metodi più utilizzati dagli hacker per introdursi nelle reti aziendali".

Il dovere di tutti

Per questo motivo, per sfruttare i vantaggi del lavoro ibrido a lungo termine, le organizzazioni devono fare in modo che la sicurezza sia un dovere costante di tutti i membri dell'azienda, e non semplicemente il ruolo della funzione IT.

Scimone spiega in che modo Dell Technologies ha adottato questa filosofia all'interno della propria azienda: "Nel corso degli anni abbiamo sviluppato una cultura della sicurezza in cui forniamo ai nostri dipendenti le giuste conoscenze e la formazione necessaria affinché possano prendere le giuste decisioni.

Un programma di formazione particolare che ha avuto molto successo è stato il nostro programma di formazione sul phishing. In questo programma, mettiamo continuamente alla prova e formiamo i nostri dipendenti inviando loro e-mail di phishing simulate, in modo che acquisiscano maggiore familiarità con i comportamenti da tenere. Già nell'ultimo trimestre abbiamo osservato un numero maggiore rispetto al passato di dipendenti che hanno individuato e segnalato il test di simulazione di phishing. Queste attività di formazione sono efficaci e fanno la differenza".[17]

Naturalmente, era molto più facile ricordare ai dipendenti le loro responsabilità in materia di sicurezza, soprattutto quando si trovavano in sede, quindi, come aggiunge Scimone, è fondamentale aumentare la consapevolezza con consigli specifici relativi alle situazioni di lavoro da remoto: "...stiamo intensificando i nostri sforzi e promuovendo la consapevolezza della sicurezza e le responsabilità che i membri del team hanno, sia che si tratti di come utilizzare in modo sicuro la VPN, sia che si tratti di proteggere la rete domestica o anche di come viaggiare in modo sicuro", afferma.

Sommario

Sostenere l'istruzione con la tecnologia

Naturalmente, oltre a fornire una formazione continua, le organizzazioni devono assicurarsi che i dipendenti siano sempre supportati da soluzioni e dispositivi orientati al futuro, in grado di salvaguardare le minacce in continua evoluzione tipiche del lavoro ibrido. Quando si valuta come proteggere i dati e i dispositivi distribuiti a lungo termine, è importante adottare una visione olistica.

Le considerazioni chiave per la protezione al di sopra del sistema operativo includono: Come eseguiamo la crittografia delle informazioni sensibili e la protezione dei dati? Come stiamo prevenendo, rilevando e rimediando agli attacchi? I nostri utenti finali possono accedere in modo sicuro alle app e ai dispositivi da qualsiasi luogo? Mentre le considerazioni chiave per la protezione al di sotto del sistema operativo includono: Stiamo proteggendo le credenziali degli utenti finali? Il nostro BIOS è protetto? Stiamo proteggendo anche la privacy digitale?

In risposta, le organizzazioni devono assicurarsi di dotare i propri dipendenti di dispositivi affidabili che creino una base sicura: con livelli di protezione resilienti sopra e sotto il sistema operativo che rafforzano la superficie di attacco dell'endpoint e proteggono, rilevano e rispondono alle minacce in evoluzione.

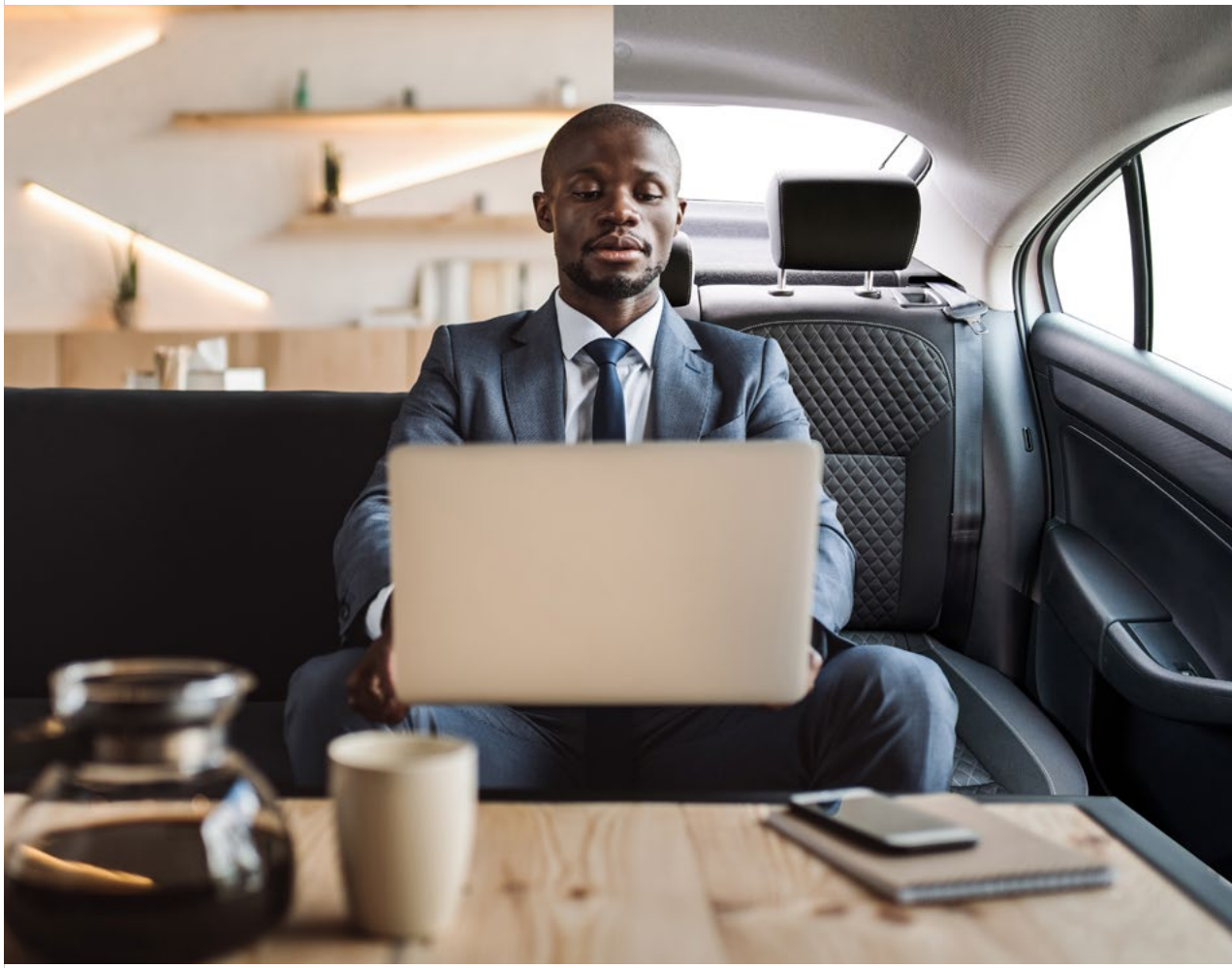
In un mondo caratterizzato da normative sempre più stringenti sulla conformità dei dati in tutti i settori e in tutte le aree geografiche, questo approccio olistico alla sicurezza del lavoro ibrido è estremamente significativo. Ad esempio, una ricerca condotta da ESG del 2022 ha rilevato che le organizzazioni preparate hanno il 44% di probabilità in più di non registrare perdite di dati dovute alla violazione di un dispositivo negli ultimi 12 mesi, con evidenti vantaggi finanziari e di conformità.[18]

Solo attraverso la formazione, sostenuta dall'azione, le aziende possono lanciarsi nel futuro del lavoro ibrido con vera fiducia e ottenere un chiaro vantaggio competitivo rispetto ai concorrenti che non hanno ancora fatto lo stesso.

> "Stiamo effettuando continui test e corsi di formazione ai nostri dipendenti inviando loro email di phishing simulate, in modo da far loro acquisire maggiore familiarità con i comportamenti da tenere".
>
> **John Scimone**, Senior Vice President e Chief Security Officer, Dell Technologies

Sommario

6 Consulenza e supporto



Sommario

Il lavoro non è più un luogo da raggiungere. Le esperienze di lavoro ibride, sicure e senza interruzioni, sono un prerequisito per la produttività dei dipendenti e per una crescita aziendale ottimale. Grazie alle nostre soluzioni all'avanguardia, alla profonda esperienza e alla scala globale, Dell Technologies e Intel sono i partner digitali affidabili per supportare le aziende a trarre il massimo vantaggio per l'azienda da questo cambiamento fondamentale dell'ambiente di lavoro.

Mobile computing

La nostra infrastruttura digitale sicura e orientata al futuro, i nostri dispositivi moderni e la nostra esperienza di supporto consentono di mantenere la privacy dei dati sensibili e di offrire un'esperienza utente moderna, essenziale per l'innovazione e la collaborazione.

Ad esempio, i moderni dispositivi di Dell Technologies, basati su Intel, aiutano a proteggere le risorse digitali e a mantenere la riservatezza dei dati sensibili grazie alla suite più completa al mondo di funzionalità intelligenti per la privacy. Livelli di protezione resilienti, sopra e sotto il sistema operativo, rafforzano la superficie di attacco dell'endpoint e aiutano a garantire la protezione, il rilevamento e la risposta alle minacce informatiche in rapida evoluzione.

Intel Hardware Shield, ad esempio, è incluso in tutti i dispositivi commerciali Dell che girano sulla piattaforma Intel vPro® e offre funzioni di sicurezza potenziate a livello hardware che aiutano a proteggere tutti i livelli dello stack di elaborazione fin dal primo utilizzo.

I dipendenti di tutto il mondo stanno ridisegnando il futuro del lavoro e, insieme a Dell Technologies e Intel, puoi assicurarti che questa nuova era di lavoro ibrido sia anche una nuova ed entusiasmante opportunità di crescita per la tua azienda.

Riferimenti

1 https://www.statista.com/statistics/1111394/attitudes-on-remote-work-for-employees/#:~:text=In%20general%2C%20employees%20consider%20remote,company%20for%20a%20remote%20role.

2 https://blogs.lse.ac.uk/businessreview/2021/09/29/remote-work-can-boost-productivity-and-curb-burnout/#:~:text=Overall%2C%20compared%20to%20those%20without,likely%20to%20report%20feeling%20included.

3 https://www.1e.com/resources/report/gartner-innovation-insight-for-the-digital-employee-experience-dex/thank-you/?submissionGuid=ZwbrOIKg21dUNdg2ONjZ

4 https://www.cnbc.com/2022/02/04/companies-are-reinventing-rules-as-employees-seek-remote-work-and-flexible-hours.html

5 https://www.cnbc.com/2022/02/04/companies-are-reinventing-rules-as-employees-seek-remote-work-and-flexible-hours.html

6 https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/vb-hybrid-work-productivity-and-collaboration-research.pdf

7 https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/dell-empowering-the-future-of-work.pdf

8 https://www.vmware.com/resources/security/global-security-insights-report-2021-index.html

9 https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/

10 eBook di ESG commissionato da Dell Technologies, "How to Build a Cyber-Resilient Business Ready to Innovate and Thrive", marzo 2022

11 Riepilogo della ricerca condotta da ESG commissionato da Dell Technologies, "Cyber Resiliency and End-User Performance", marzo 2022

12 https://www.pwc.com/gx/en/news-room/press-releases/2021/pwc-future-of-work-survey-2021.html

13 Riepilogo della ricerca condotta da ESG commissionato da Dell Technologies, "Cyber Resiliency and End-User Performance", marzo 2022

14 eBook di ESG commissionato da Dell Technologies, "How to Build a Cyber-Resilient Business Ready to Innovate and Thrive", marzo 2022

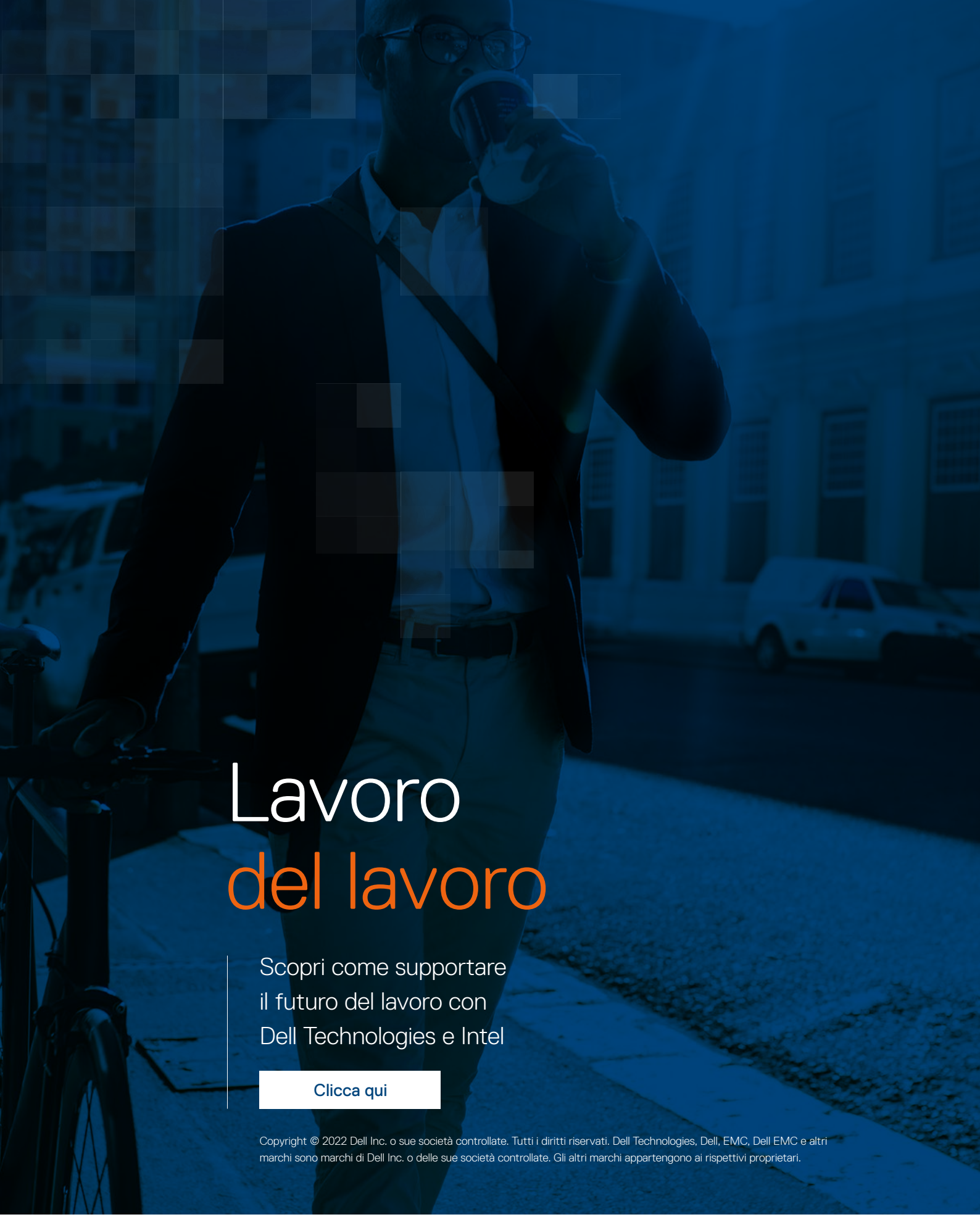
15 eBook di ESG commissionato da Dell Technologies, "Organizations Accelerating Their Digital Workplace Achieve Improvements", aprile 2021

16 https://www.walesonline.co.uk/news/uk-news/brits-admit-spying-what-fellow-23734428

17 https://www.technologyreview.com/2021/11/22/1040358/security-is-everyones-job-in-the-workplace/

18 Riepilogo della ricerca condotta da ESG commissionato da Dell Technologies, "Cyber Resiliency and End-User Performance", marzo 2022

Sommario



Lavoro del lavoro

Scopri come supportare il futuro del lavoro con Dell Technologies e Intel

Clicca qui

Copyright © 2022 Dell Inc. o sue società controllate. Tutti i diritti riservati. Dell Technologies, Dell, EMC, Dell EMC e altri marchi sono marchi di Dell Inc. o delle sue società controllate. Gli altri marchi appartengono ai rispettivi proprietari.

DELL Technologies

Innovation Built-In intel