

I vantaggi del consolidamento dell'IT



Indice

01

Espansione dell'IT
fuori controllo



02

Niente più soluzioni
disconnesse per il team IT



03

Il potere dell'unità



04

Protezione
dell'utilizzo dell'IA



05

Piattaforma
unificata



06

All'avanguardia con il
consolidamento dell'IT



L'opportunità di consolidamento dell'IT

Questo e-Book è destinato ai leader IT che sono stufi di gestire una situazione caotica e desiderano portare armonia nella loro infrastruttura IT, nella gestione e tra i dipendenti. Scopri come migliorare le performance, ridurre la complessità e i costi, aumentare l'efficienza, rafforzare la sicurezza e preparare l'organizzazione per l'intelligenza artificiale attraverso il consolidamento in una piattaforma unificata.

01

Espansione dell'IT fuori controllo

Quando si tratta di gestire un ecosistema digitale, il controllo unificato può sembrare fuori portata. **Per soddisfare le esigenze in evoluzione dell'organizzazione in termini di produttività, sicurezza e preparazione per l'IA, spesso è necessario combinare le soluzioni insieme, uno strumento alla volta.** Sebbene questo approccio garantisca la produttività, crea anche un sistema IT complesso che sovente è disconnesso, dispendioso in termini di tempo e costoso da mantenere.

I team IT possono rapidamente essere sopraffatti da questo complesso e spesso costoso set di strumenti per la gestione degli endpoint, la gestione delle identità e degli accessi, la messaggistica, l'e-mail e la produttività. E non è tutto. Diversi strumenti sovente significano fornitori diversi con requisiti unici e ambienti isolati. Non sorprende che i budget e le risorse sembrino essere al limite.

La complessità crea sfide per l'intera organizzazione. La produttività si blocca quando i dipendenti trascorrono la giornata effettuando più accessi e cercando di condividere informazioni tra strumenti disconnessi. Nel tentativo di accedere alle risorse da dispositivi e posizioni differenti, la gestione frammentata degli endpoint rende più difficile per i team IT garantire la sicurezza. È il momento di unificare gli strumenti IT e semplificare la gestione.

L'ecosistema di fornitori e strumenti IT specializzati continua a crescere, rapidamente.



Niente più tassa sulla complessità

Ogni licenza software nuova segue un modello simile: un'altra soluzione, un altro centro di costo, un altro livello di complessità. Ai leader IT viene chiesto di fare molto con un budget limitato e in qualche modo devono ancora trovare le risorse per supportare nuove iniziative di IA. Per tenere il budget sotto controllo, molti responsabili IT devono valutare costantemente la propria infrastruttura alla ricerca di licenze duplicate e inutilizzate. Nel 2024, i leader IT hanno ottenuto risparmi nei modi seguenti:

83% ha ridotto la spesa per software inutilizzato²

82% ha migliorato la negoziazione dei contratti con i fornitori²

79% ha acquistato licenze meno costose²

Queste strategie possono comportare risparmi moderati. Ma c'è un problema. La gestione di questa crescente combinazione di applicazioni crea una "tassa sulla complessità". Occorrono personale e tempo prezioso per controllare gli strumenti e rimuovere le funzionalità inattive, gestendo al tempo stesso le impostazioni di sicurezza e accesso per le soluzioni disconnesse. Aniché concentrarsi sulle attività ad alto impatto, i team IT dedicano tempo importante a controllare le licenze, a negoziare con i fornitori e a conseguire risparmi incrementali, mantenendo contemporaneamente ogni soluzione esistente. Queste attività dispendiose in termini di tempo sottraggono l'attenzione ad attività più significative.

Nonostante queste misure di riduzione dei costi, la tassa sulla complessità torna ad aumentare. L'unico percorso sostenibile futuro è quello di ridefinire l'approccio tecnologico. Il consolidamento in una piattaforma completa ridurrà la complessità e consentirà ai team di concentrarsi sulla trasformazione del business.

15%

delle organizzazioni ha pagato più di 5 milioni di USD per gli **audit dei fornitori di software** negli ultimi tre anni²

61%

dei professionisti della gestione delle risorse IT afferma di **non avere ancora una visibilità completa** sulle risorse IT che influiscono sui risultati aziendali²

02

Niente più soluzioni disconnesse per il team IT

Per le organizzazioni con un'ampia gamma di offerte tecnologiche, la realtà quotidiana delle attività IT è estenuante. Ogni soluzione monouso richiede competenze specifiche. L'ecosistema tecnologico si trasforma in un intricato labirinto di strumenti disconnessi.

I team IT sono sovraccaricati di tutte le attività di gestione, manutenzione, integrazione e supporto. Ogni strumento specializzato richiede una gestione diretta. Pertanto sono necessari più specialisti con competenze specifiche solo per mantenere operativi i sistemi. Ormai il **64%** dei leader aziendali IT segnala problematiche nell'assunzione di candidati a causa della mancanza di competenze o esperienza necessarie.³ Ciò significa che è più difficile assumere, eseguire l'onboarding e mantenere le conoscenze approfondite dei membri del team.



03

Il potere dell'unità

Esiste un approccio migliore alla gestione IT. Consolidando una soluzione unificata, puoi ridurre il sovraccarico dell'IT e mantenere un team forte, flessibile e concentrato. In questo modo puoi:

Ottimizzare la gestione della negoziazione dei contratti, della manutenzione e delle operazioni dei fornitori

Migliorare la produttività accelerando il supporto e la gestione delle richieste

Proteggere in modo proattivo l'ambiente IT con una visibilità e una gestione unificate

Non è solo una questione di semplificare i sistemi. Si tratta di aprire la strada per ciò che conta di più: consentire al team di plasmare il futuro del funzionamento dell'organizzazione.

Riduzione al minimo degli attriti digitali

La tecnologia deve aiutare a spianare la strada, non creare ostacoli. In qualità di leader IT, sai che la **disconnessione tra strumenti di produttività influisce sull'intera organizzazione**.

Il **62%** delle persone afferma di dedicare troppo tempo alla ricerca di informazioni nell'arco della giornata lavorativa.⁵ Il dipendente medio ora trascorre il **57%** della giornata lavorativa in riunioni, scrivendo e-mail e conversando in chat. Pertanto non sorprende che il **68%** delle persone sostenga di non riuscire a garantire la produttività senza interruzioni.⁵

Le soluzioni mirate disconnesse creano resistenza nei flussi di lavoro quotidiani in modo discreto, ma la frustrazione aumenta rapidamente. Accessi multipli, attività isolate, informazioni sparse, sistemi che non funzionano insieme: ogni punto di attrito è una piccola tassa sulla creatività e sull'innovazione.

Grazie al consolidamento in un'unica piattaforma, puoi ridurre queste barriere e trovare lo spazio in cui può emergere la creatività di valore. Immagina la tua organizzazione trasformata dal consolidamento. I lavoratori utilizzano un gateway centrale e sicuro per accedere a tutti gli strumenti e le risorse di cui hanno bisogno. Le informazioni fluiscono liberamente e la collaborazione avviene in modo naturale.

Quando l'attrito scompare, le persone riscoprono la loro capacità di lavorare in modo più significativo. Non si tratta solo di superare gli ostacoli, ma di creare un ambiente in cui la tecnologia amplifichi ciò che le persone possono fare.



Centralizzazione della sicurezza

Il panorama delle minacce informatiche è più complesso che mai. Gli utenti malintenzionati dispongono di risorse migliori, sono più sofisticati e hanno tattiche che mettono alla prova anche i team addetti alla sicurezza più preparati. Man mano che le minacce per la sicurezza diventano più sofisticate, tenere il passo è più difficile. L'**80%** delle organizzazioni ha percorsi di attacco che espongono risorse critiche.⁶ L'**82%** dei leader della sicurezza è stato sorpreso da un incidente di sicurezza che ha eluso un controllo che pensavano fosse in atto.⁷

Le organizzazioni ora spendono il **65%** del budget destinato alla sicurezza per prodotti di terze parti, mentre solo il **35%** va alla manodopera interna.⁸

Cosa porta a questa spesa sbilanciata? Le grandi aziende spesso gestiscono una vasta gamma di strumenti per assicurarsi di avere la soluzione migliore per ogni attività specifica, anche quando ciò significa destreggiarsi tra una suite più ampia. Questo approccio può portare a un aumento delle spese e della complessità.

600 Mio

di attacchi di criminalità informatica si sono verificati quotidianamente nel 2024⁶

2,75x

di aumento anno dopo anno degli episodi collegati al ransomware gestito da esseri umani⁶

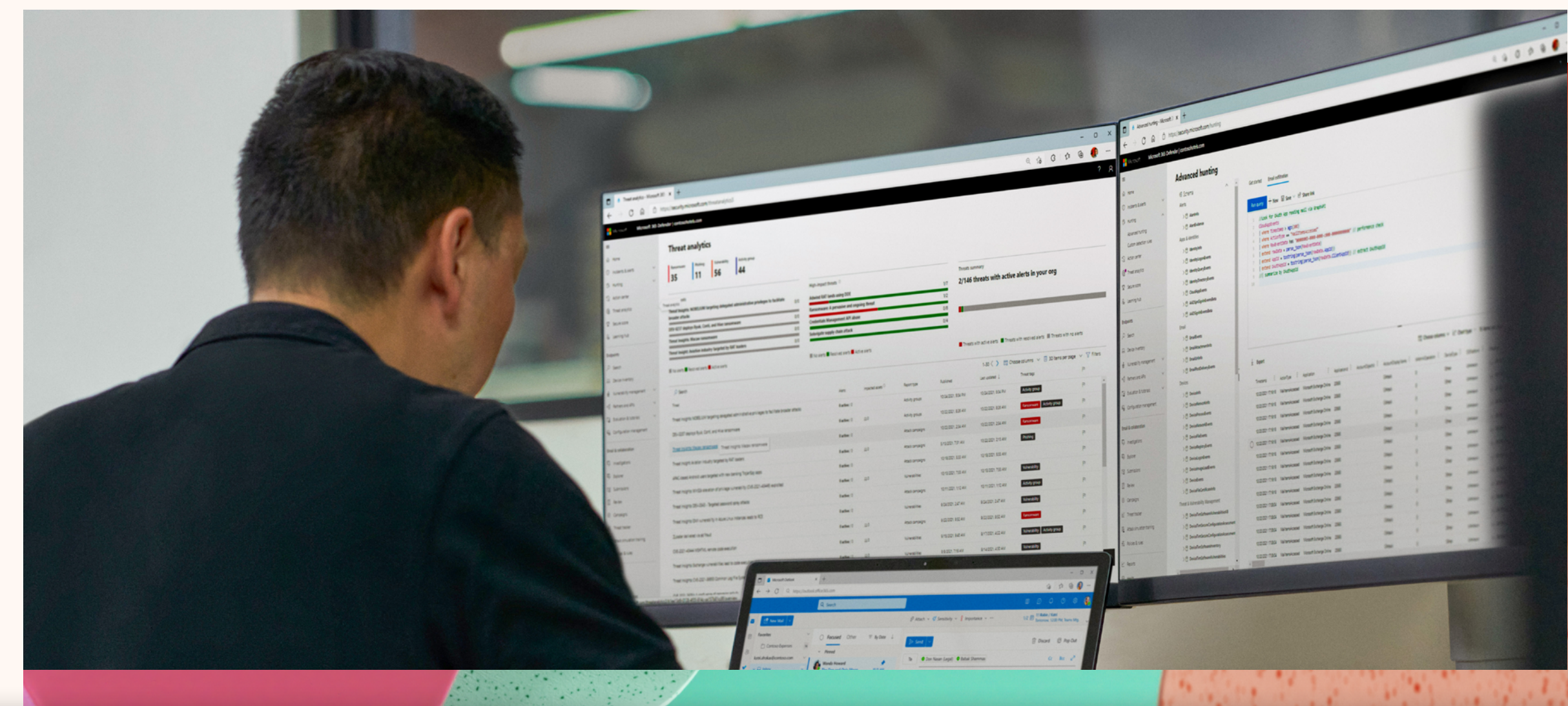
In risposta all'aumento delle minacce, i team addetti alla sicurezza aggiungono altre soluzioni.

19%

di aumento medio nel corso di due anni del numero di strumenti di sicurezza utilizzati dalle grandi aziende⁷

L'aggiunta di ulteriori strumenti di sicurezza può sembrare una difesa più efficace per l'organizzazione. Tuttavia la ricerca di una soluzione può effettivamente renderla più vulnerabile. Un ambiente IT complesso, con molte interdipendenze, è più difficile da comprendere, gestire e proteggere. Il sovraccarico di strumenti impedisce di ottenere una visione chiara, a livello aziendale, dello stack tecnologico completo. Crea anche un'altra superficie di attacco potenziale con più "accessi secondari" nei sistemi aziendali.

Consolidando la protezione in una piattaforma completa, puoi sciogliere la complessità. In questo modo ottieni una visione chiara dell'intero patrimonio digitale. La postura di sicurezza migliore non si trova in una crescente raccolta di strumenti distinti. La raggiungi quando getti le basi giuste con una piattaforma centrale.



04

Protezione dell'utilizzo dell'IA

I dipendenti non vedono l'ora che l'IA alleggerisca il loro lavoro.

75% dei dipendenti **sta già usando l'IA** al lavoro⁹

78% dei lavoratori che usano l'IA **porta già i propri strumenti di IA** al lavoro⁹

I dipendenti non hanno intenzione di aspettare che i protocolli di sicurezza si adeguino. Con l'aumento della popolarità degli strumenti "Bring Your Own AI" (BYOAI), le organizzazioni rischiano di rimanere indietro. Solo il **24%** delle iniziative di IA generativa include misure di sicurezza robuste.¹⁰

Se le organizzazioni non creano le basi giuste per un utilizzo sicuro dell'intelligenza artificiale, i dipendenti potrebbero colmare il divario di produttività con la shadow IA: strumenti non approvati che esistono fuori dai sistemi e fuori dal tuo controllo.

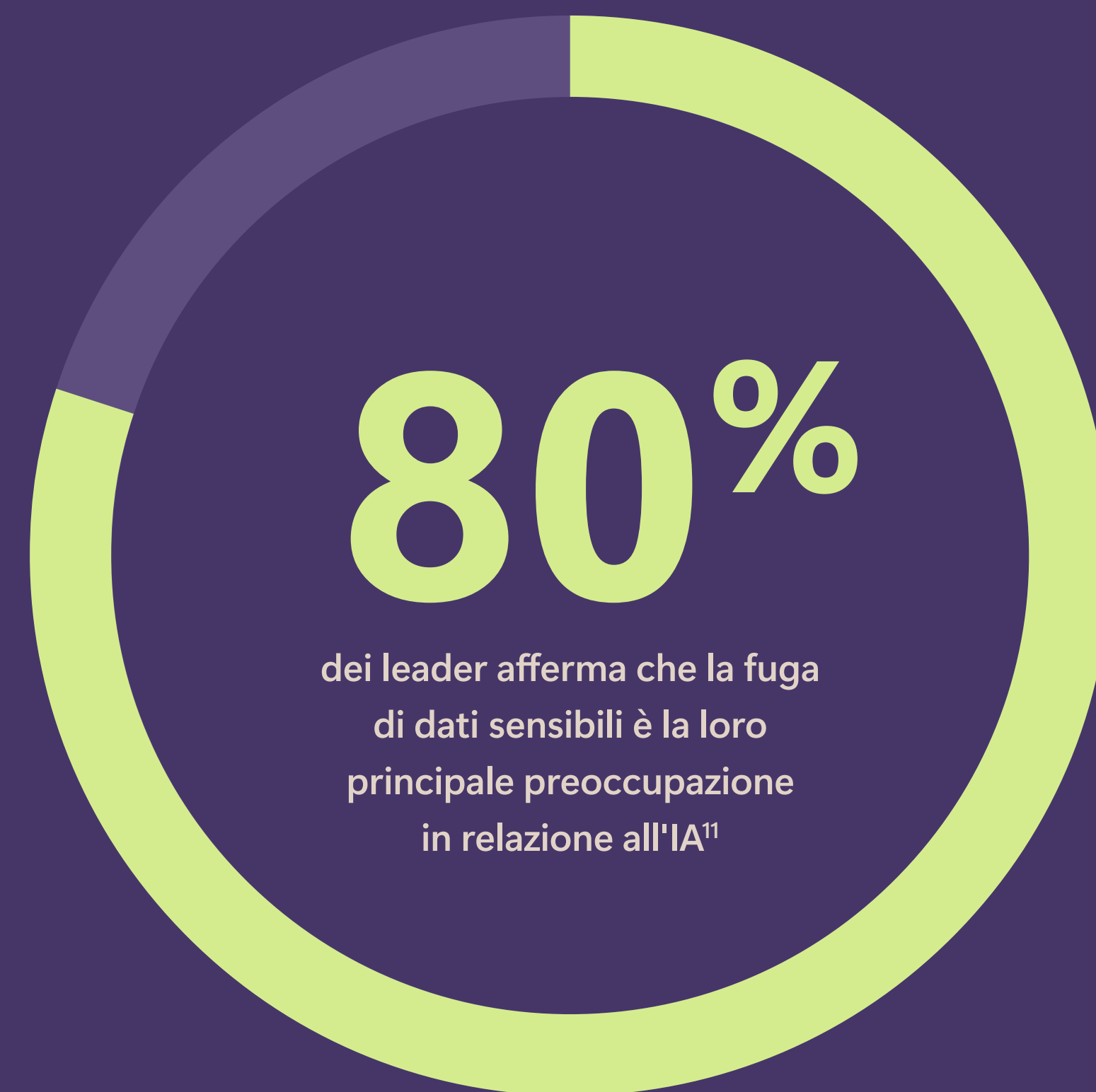
La shadow IA comporta due sfide principali:

Senza supervisione

La shadow IA comporta rischi seri. Cosa impedisce ai dipendenti di copiare e incollare informazioni sensibili nel proprio strumento personale di intelligenza artificiale? Ogni interazione con i dispositivi BYOAI non controllati diventa un'altra minaccia per la sicurezza. È probabile che i tuoi dati finiscano per essere divulgati o vengano utilizzati per sottoporre a training un modello esterno.

Utilità limitata

Il **79%** dei dipendenti si sentirebbe a proprio agio nell'utilizzo dell'intelligenza artificiale per attività analitiche,⁵ ma uno strumento di IA è valido solo quanto le informazioni cui può accedere. Gli strumenti di intelligenza artificiale segmentati e isolati forniscono spesso risposte incomplete. Ecco perché gli strumenti BYOAI hanno solo un'utilità limitata per i lavoratori.





Ora le organizzazioni si trovano a un bivio: lasciare che l'utilizzo frammentato dell'IA aumenti vertiginosamente gli incidenti di sicurezza potenziali o assumere il controllo e adottare una piattaforma unificata pronta per l'IA. In qualità di leader IT, hai un'importante opportunità strategica per guidare la tua organizzazione in questo momento critico. Sfrutta appieno la potenza dell'intelligenza artificiale nell'intera organizzazione con una suite aziendale che riunisce applicazioni per la produttività e funzionalità di sicurezza e compliance, il tutto progettato per una perfetta integrazione dell'IA.

Una piattaforma consolidata consente di distribuire in modo efficace gli strumenti giusti per ridurre i rischi legati all'utilizzo dell'intelligenza artificiale e proteggere i dati. Il consolidamento contribuisce inoltre a distribuire e gestire meglio una connessione semplice e sicura tra la soluzione di intelligenza artificiale della tua organizzazione e i dati, le risorse e i flussi di lavoro proprietari. In questo modo la tua soluzione di intelligenza artificiale fornisce ai dipendenti gli insights fruibili e accurati di cui hanno bisogno per portare a termine attività di grande impatto.

Piattaforma unificata

Microsoft 365 E3 è una piattaforma unificata che semplifica la gestione IT, migliora la produttività dell'organizzazione con esperienze connesse, fornisce strumenti ed endpoint e si integra perfettamente con l'intelligenza artificiale.

I vantaggi del consolidamento con Microsoft 365 E3

Riduzione dei costi dell'IT

Scegli una soluzione completa che semplifichi la gestione dal cloud e consolidi i fornitori per ridurre al minimo i costi totali e migliorare il ROI.

Protezione dell'organizzazione

Proteggi l'accesso a dati, applicazioni e risorse con una soluzione centralizzata per la protezione dalle minacce, un'autenticazione a più fattori solida, criteri di accesso condizionale e una valutazione continua dell'accesso.

Adozione sicura dell'IA generativa

Creando una base di protezione con una piattaforma completa che mantiene la privacy e la sicurezza dei dati, l'organizzazione è pronta ad adottare l'intelligenza artificiale con Microsoft 365 Copilot.

Riduzione della complessità dell'IT

Centralizza la gestione di applicazioni, endpoint e identità, riducendo al tempo stesso le soluzioni mirate per la produttività. A questo scopo controlla l'accesso e l'utilizzo senza interrompere il flusso di lavoro all'interno dell'organizzazione.

Consolidando l'ecosistema IT con Microsoft 365 E3, stai scegliendo un modo di lavorare più sicuro e più produttivo. Questa piattaforma completa consente al team IT e all'intera organizzazione di affrontare qualsiasi sfida futura.

06

All'avanguardia con il consolidamento dell'IT

Il ritmo odierno della proliferazione IT non è più sostenibile. Consolidare l'ecosistema digitale non è solo una mossa strategica: è fondamentale per ridurre i costi, semplificare la gestione, accelerare la produttività e rafforzare la sicurezza. Unificando gli strumenti e i processi, consentirai all'organizzazione di lavorare in modo più efficiente, innovare più velocemente e adottare l'intelligenza artificiale in tutta sicurezza.



Inizia ora

Fonti

¹ "The state of observability in 2024", Dynatrace, 2024.
<https://www.dynatrace.com/info/reports/state-of-observability-2024/>

² "2024 State of ITAM Report", Flexera, 2024.
<https://info.flexera.com/ITAM-REPORT-State-of-IT-Asset-Management>

³ "Challenges in recruiting employees in the IT industry worldwide 2023", Statista, 5 dicembre 2023.
<https://www.statista.com/statistics/1425097/recruitment-challenges-in-the-tech-industry-worldwide/>

⁴ "Is IT Complexity Standing in the Way of Your Organization's Growth?", Harvard Business Review, 9 dicembre 2022.
<https://hbr.org/sponsored/2022/12/is-it-complexity-standing-in-the-way-of-your-organizations-growth>

⁵ "L'IA risolverà il problema del lavoro?", Microsoft Work Trend Index, 9 maggio 2023.
<https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>

⁶ "Report sulla difesa digitale Microsoft 2024", Microsoft Security, 2024.
<https://www.microsoft.com/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024>

⁷ "2022 Security Leaders Peer Report", Panaseer, 2022.
<https://panaseer.com/resources/reports/2022-security-leaders-peer-report>

⁸ "The cybersecurity provider's next opportunity: Making AI safer", McKinsey & Company, 14 novembre 2024.
<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer>

⁹ "L'IA è arrivata al lavoro. Ora inizia la parte difficile", Microsoft Work Trend Index, 8 maggio 2024.
<https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>

¹⁰ "Cost of a Data Breach Report 2024", IBM, 2024.
<https://www.ibm.com/reports/data-breach>

¹¹ "La sicurezza dei dati come base per un'adozione sicura dell'intelligenza artificiale", Microsoft Security, 2024.
<https://clouddamcdnprodep.azureedge.net/gdc/gdckHueRY/original>

©2025 Microsoft Corporation. Tutti i diritti sono riservati. Il presente documento viene fornito "così com'è". Le informazioni e le opinioni in esso contenute, inclusi gli URL e altri riferimenti a siti Web Internet, possono variare senza preavviso. Qualsiasi rischio correlato all'uso del documento è a carico dell'utente. Questo documento non garantisce alcun diritto legale sulla proprietà intellettuale di alcun prodotto Microsoft. Il presente documento può essere copiato e usato esclusivamente per scopi interni e di riferimento.