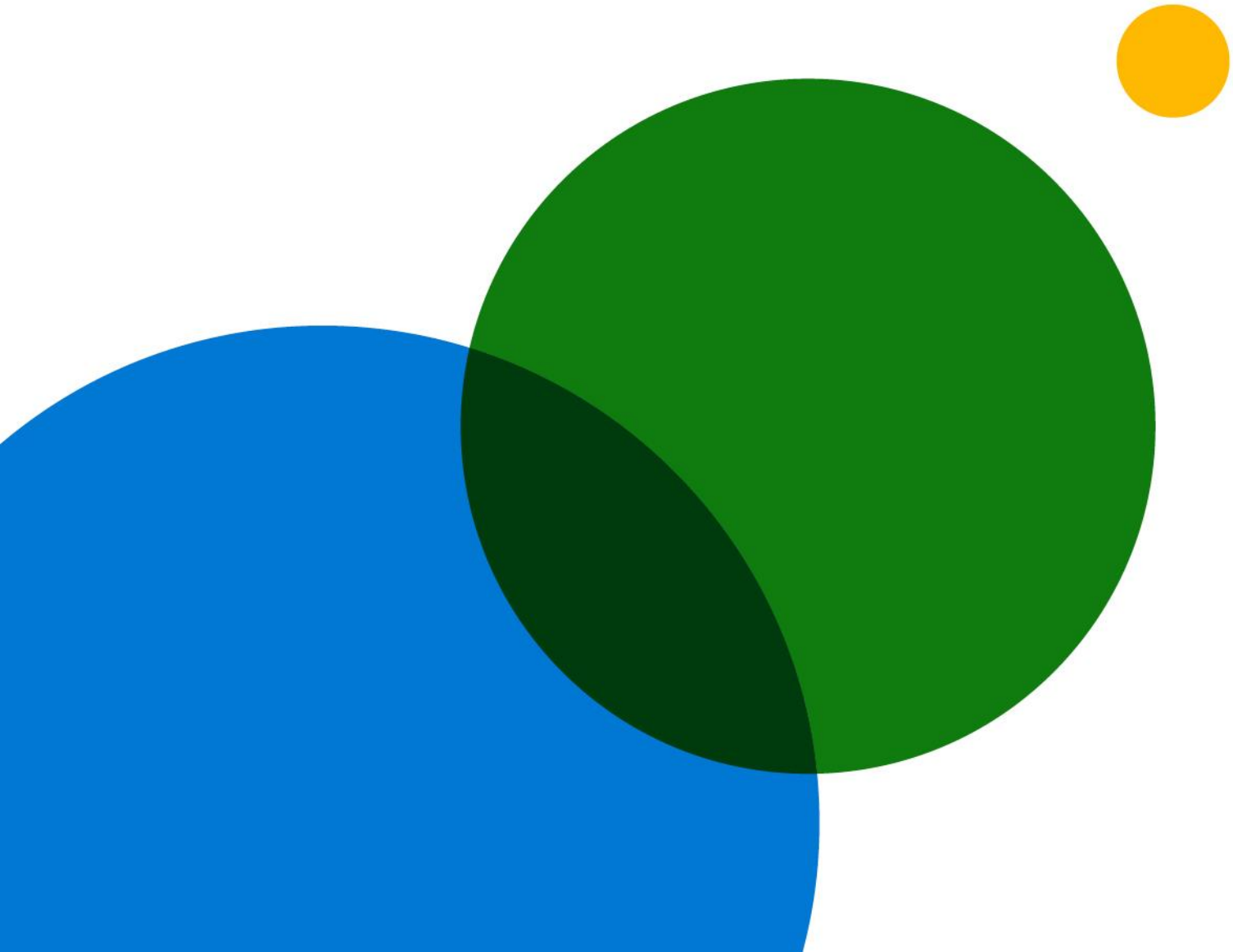
Microsoft Security

hypothesis

# Report sull'adozione di Zero Trust



# Indice

# Presentazione

Vasu Jakkal / Corporate Vice President, Sicurezza, adeguamento e identità

L'anno scorso è stato straordinario per l'evolvere della sicurezza informatica e l'ascesa di Zero Trust come strategia guida per il settore e le aziende in tutto il mondo.

All'inizio della pandemia, l'ambiente di lavoro è diventato quasi completamente remoto dalla sera alla mattina. Questo cambiamento ha costretto molte aziende ad adattarsi rapidamente per supportare i dipendenti che lavoravano in qualsiasi modo possibile, con dispositivi personali, collaborando tramite i servizi cloud e condividendo dati al di fuori del perimetro della rete aziendale. Mentre le aziende si adattavano a questa trasformazione, hanno dovuto inoltre affrontare criminali informatici sempre più sofisticati i cui obiettivi, tattiche e risorse cambiavano continuamente.

Oggi il lavoro ibrido è la nuova realtà. In questo contesto, e di fronte al rapido cambiamento, le aziende che abbiamo intervistato ci hanno detto che si affidano a Zero Trust per potenziare la sicurezza, essere agili nell'adeguamento, rilevare e rimediare alle minacce più rapidamente e aumentare la semplicità e disponibilità delle analisi di sicurezza.

L'architettura Zero Trust a 360 gradi, basata sui principi della verifica esplicita, sull'accesso con privilegi minimi e sulla presunzione di violazione, crea protezioni all'interno e tra identità, endpoint, app, infrastrutture, reti e dati, collaborando con maggiore visibilità, automazione e orchestrazione. Non solo consigliamo questo approccio ai nostri clienti e partner, ma lo adottiamo come nostro approccio alla sicurezza globale e allo sviluppo di software in Microsoft.

Questo report illustra il percorso di adozione del modello Zero Trust in diversi mercati e settori. Ci auguriamo che le conoscenze acquisite con questa ricerca possano accelerare la tua adozione della strategia Zero Trust, far luce sul progresso collettivo dei tuoi colleghi e fornire informazioni particolareggiate sullo stato futuro di questo ambito in rapida evoluzione.

# Metodologia

Microsoft ha commissionato a Hypothesis Group, un'agenzia di analisi, progettazione e strategia, l'esecuzione il Report sull'adozione del modello Zero Trust e la relativa ricerca. La ricerca prevedeva due fasi negli Stati Uniti per evidenziare le tendenze e lo slancio nell'adozione del modello Zero Trust, con l'aggiunta di altri mercati nella seconda fase per scoprire le tendenze globali.

La fase iniziale della ricerca si è svolta ad agosto 2020, con un sondaggio online di 15 minuti negli Stati Uniti rivolto a 300 decisori per la sicurezza coinvolti nelle decisioni sulla strategia Zero Trust in aziende di diversi settori. Oltre al sondaggio online, a settembre 2020 sono state condotte cinque interviste approfondite tra decisori per la sicurezza statunitensi di vari settori.

Ad aprile 2021 si è svolta una ricerca globale negli Stati Uniti, in Germania, Giappone e Australia/Nuova Zelanda, rivolta a un gruppo analogo di decisori per la sicurezza. Oltre 900 partecipanti hanno risposto a un sondaggio online di 15 minuti con domande sull'adozione della strategia Zero Trust, procedure consigliate, vantaggi, sfide e su come intendono investire in futuro.

# Cose da sapere sull'adozione di Zero Trust

### 01 / Le aziende sono pronte a trarre vantaggio dalla strategia Zero Trust, accelerata dal passaggio a un ambiente di lavoro ibrido e dal Covid-19

I responsabili delle decisioni per la sicurezza sostengono che lo sviluppo di una strategia Zero Trust è la loro priorità di sicurezza numero 1 e il 96% afferma che essa è fondamentale per il successo dell'azienda. I motivi principali dell'adozione della strategia Zero Trust sono migliorare l'approccio generale alla sicurezza e l'esperienza degli utenti finali. Il passaggio a un ambiente di lavoro ibrido, accelerato dal COVID-19, sta inoltre promuovendo l'adozione della strategia Zero Trust: l'81% delle aziende ha iniziato la migrazione a un ambiente di lavoro ibrido e il 31% di esse l'ha già completata. Il 94%, però, esprime preoccupazione riguardo alla transizione, principalmente per le procedure non corrette dei dipendenti, l'aumento dei workload IT e gli attacchi informatici. Alla luce di ciò, le principali considerazioni strategiche includono una maggiore formazione dei dipendenti e l'autenticazione a più fattori (MFA) per garantire un'esperienza utente e una transizione fluide.

### 02 / La strategia Zero Trust offre flessibilità relativamente alle aree da cui le aziende possono iniziare l'implementazione, pertanto l'approccio possa essere modulato sulle loro esigenze

Meno del 15% delle aziende ha iniziato a implementare la strategia Zero Trust nella stessa area a rischio sicurezza. Ciò dipende in gran parte dal fatto che l'implementazione viene affrontata come un processo end-to-end tra pilastri e caratteristiche dell'architettura di sicurezza, anziché come una serie di tecnologie disparate e singole. Analogamente, l'ordine di implementazione dei singoli componenti di Zero Trust in un'area a rischio sicurezza è molto variabile, con notevoli differenze tra i professionisti della sicurezza quanto alla decisione dei componenti da implementare per primi.

### 03 / Sebbene la strategia Zero Trust sia ampiamente adottata e migliori la capacità delle aziende di gestire le minacce, c'è ancora molto da fare

Il 76% delle aziende ha almeno iniziato a implementare la strategia Zero Trust, mentre il 35% dichiara di averla completamente implementata. Tuttavia, queste ultime aziende ammettono di non aver completato l'implementazione della strategia Zero Trust in tutte le aree e i componenti a rischio. La strategia Zero Trust è interessante perché offre una maggiore agilità, velocità di rilevamento delle minacce e una migliore capacità di gestire la sicurezza dell'Internet delle Cose (IoT) e della tecnologia operativa (OT). L'adozione sta crescendo negli Stati Uniti (dal 70% ad agosto 2020 al 79% ad aprile 2021); gli Stati Uniti sono inoltre in anticipo nell'implementazione del modello Zero Trust rispetto ad altri paesi che hanno iniziato il percorso di adozione successivamente e le aziende negli Stati Uniti dichiarano di avere meno vincoli di budget. Tuttavia, mentre il 57% delle aziende sostiene di essere a buon punto nel percorso di adozione, circa la metà deve lavorare ancora molto perché non ha implementato completamente il modello Zero Trust in tutte le aree e i componenti a rischio sicurezza.

### 04 / Guardando al futuro, la strategia Zero Trust rimarrà una priorità assoluta e richiederà un processo decisionale attento per quanto riguarda dipendenti e fornitori

È probabile che la strategia Zero Trust rimarrà la priorità di sicurezza numero 1 tra due anni e le aziende prevedono di aumentare i loro investimenti. Superare le sfide dei dipendenti (inclusa la formazione di team di sicurezza e l'approvazione da parte della leadership) sarà un fattore chiave per raddoppiare l'investimento nella strategia Zero Trust. Quanto alla strategia fornitori, i decisori per la sicurezza preferiscono lavorare con fornitori generali o consolidati perché la selezione dei fornitori dipende spesso dalla disponibilità di competenze interne. L'approccio del fornitore unico presenta alcuni vantaggi, come livelli maggiori di competenza e risorse e una maggiore semplicità, ma può richiedere un tempo di implementazione più lungo, essere più difficile da integrare con l'architettura di sicurezza esistente e aumentare la potenziale vulnerabilità.

# Con chi abbiamo parlato

Globale


* Più di 1.000 dipendenti negli Stati Uniti; oltre 500 dipendenti in Germania, Giappone, Australia/Nuova Zelanda

# Risultati generali della ricerca

# Le aziende sono pronte a trarre vantaggio dalla strategia Zero Trust

Oggi la strategia Zero Trust è la massima priorità per la sicurezza in tutti i mercati e settori e numerose aziende hanno adottato la strategia Zero Trust negli ultimi anni. Pur essendo importante in tutti i paesi (53%), questa strategia rappresenta una massima priorità per le aziende degli Stati Uniti (56%) e della Germania (53%).

Quasi tutti i professionisti della sicurezza (96%) ritengono che una strategia Zero Trust sia fondamentale per il successo dell'azienda (Figura 1). Oltre che per rafforzare il livello generale di sicurezza e l'esperienza degli utenti finali, i professionisti della sicurezza si rivolgono alla strategia Zero Trust per semplificare le procedure di sicurezza per i dipendenti (Figura 2).

Un decisore statunitense per la sicurezza nel settore dei servizi di ospitalità spiega: *"L'obiettivo è migliorare il nostro approccio generale alla sicurezza, ma riducendo l'attrito nell'esperienza dell'utente finale e semplificando la vita degli utenti"*.

Inoltre, il 31% dei professionisti della sicurezza considera la strategia Zero Trust uno strumento importante per l'imminente passaggio a un luogo di lavoro ibrido post pandemia; questo fattore è particolarmente rilevante in Australia/Nuova Zelanda (44%).

**Figura 1. Zero Trust è fondamentale**

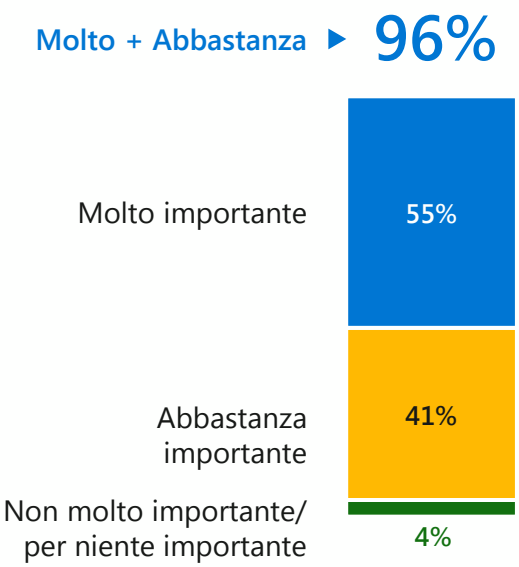



**Figura 2. Motivazioni Zero Trust**

| Motivazioni principali | |
|---|---|
| Migliorare l'approccio complessivo alla sicurezza | 47% |
| Migliorare l'esperienza e produttività degli utenti finali | 44% |
| Trasformare le modalità di collaborazione dei team della sicurezza | 38% |
| Semplificare lo stack di sicurezza | 35% |
| Ridurre i costi per la sicurezza | 35% |

# Il passaggio a un ambiente di lavoro ibrido favorisce una maggiore adozione della strategia Zero Trust

L'81% delle aziende ha iniziato la transizione verso un ambiente di lavoro ibrido e il 31% ha già completato l'adozione. Detto questo, i tassi di adozione completa differiscono da mercato a mercato: mentre l'Australia e la Nuova Zelanda sono al comando con il 37%, la Germania è molto indietro, con appena il 20% delle aziende già transitate a un modello ibrido (Figura 3).

Anche se i mercati globali stanno passando a un ambiente di lavoro ibrido a ritmi diversi, la stragrande maggioranza (91%) delle aziende che non ha completato la transizione prevede di farlo nei prossimi cinque anni. Fondamentalmente, il 94% è preoccupato per la transizione: uso non corretto da parte dei dipendenti, aumento dei workload IT e un rischio maggiore di attacchi informatici costituiscono le principali preoccupazioni (Figura 4).

**Figura 3. Verso un ambiente di lavoro ibrido**

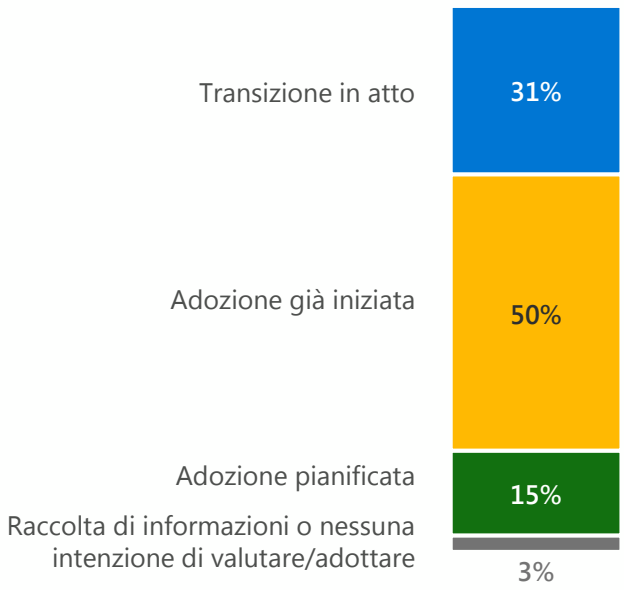
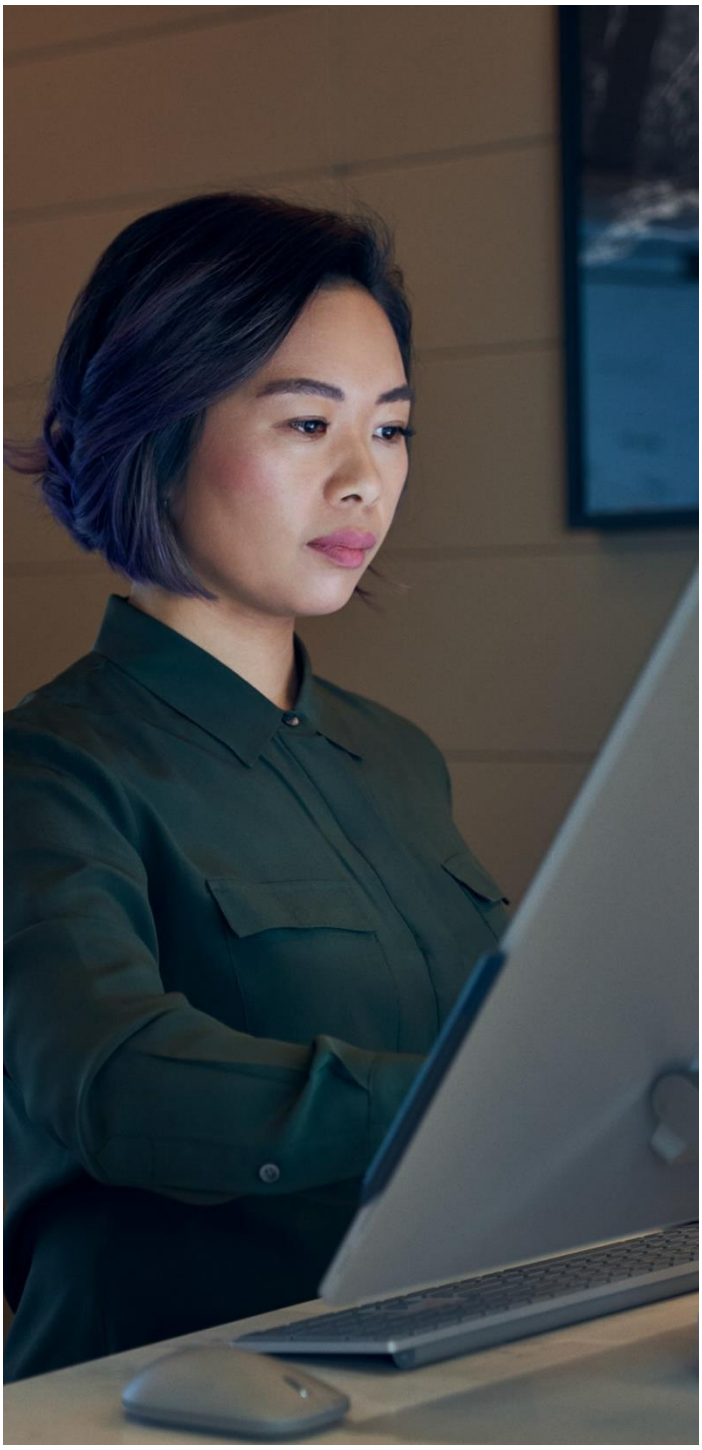



**Figura 4. Dubbi sull'ambiente di lavoro ibrido**

| | |
|---|---|
| Dipendenti che scaricano app non sicure | 37% |
| Aumento del workload IT | 37% |
| Attacchi ransomware | 36% |
| Attacchi di phishing | 35% |
| Uso non corretto dei dispositivi personali | 34% |
| Accesso non autorizzato ai dati | 31% |
| Impossibilità di gestire tutti i dispositivi | 30% |
| Uso di account e-mail personali | 30% |
| Mancato adeguamento alle normative sui dati | 24% |

# Il Covid-19 ha fatto nascere nuove considerazioni che accelerano il passaggio alla strategia Zero Trust



Nel tentativo di ridurre al minimo i potenziali problemi, le parti interessate sottolineano l'importanza di una maggiore formazione per i dipendenti (54%) (in particolare in Giappone (61%) e Germania (58%)) e dell'autenticazione a più fattori (MFA) (50%) (in particolare negli Stati Uniti (52%) e in Germania (56%)) per garantire un'esperienza utente e una transizione fluide.

Poiché la strategia Zero Trust supporta il lavoro ibrido e remoto, il COVID-19 ne ha accelerato l'adozione nel 72% delle aziende, anche se emergono alcune differenze tra i mercati. Se da un lato la pandemia è servita da catalizzatore per l'adozione in circa sette aziende su dieci negli Stati Uniti (76%), in Giappone (71%) e in Australia/Nuova Zelanda (69%), i tassi di implementazione sono stati nettamente inferiori in Germania (62%), forse a causa di una transizione più lenta verso un ambiente di lavoro ibrido.

# Zero Trust è largamente implementato in tutto il mondo e sta crescendo negli Stati Uniti

Zero Trust non è solo un termine in voga, ma una realtà. Il 76% delle aziende ha perlomeno iniziato a implementare questa strategia e il 35% ritiene di aver completato l'implementazione. Tuttavia, questi dati tracciano un quadro eccessivamente ottimistico perché molte aziende che ritengono di aver completato l'implementazione, per loro stessa ammissione, non l'hanno terminata in tutte le area a rischio sicurezza. Oggi gli Stati Uniti sono in anticipo nell'adozione della strategia Zero Trust rispetto ad altri mercati e continuano a crescere rapidamente: rispetto ad agosto 2020, l'implementazione della strategia Zero Trust negli Stati Uniti è passata dal 70% al 79%: un balzo considerevole in soli otto mesi (Figura 5).

Sebbene la strategia Zero Trust sia attualmente predominante in ambito sicurezza, la sua adozione in tutte le aree è un relativamente recente. L'82% delle aziende ha implementato strategie Zero Trust negli ultimi tre anni (il 21% negli ultimi 12 mesi). Detto questo, il 26% delle aziende statunitensi ha iniziato l'implementazione più di 3 anni fa, rispetto al 19% delle aziende giapponesi, al 6% di quelle di Australia/Nuova Zelanda e al 3% delle aziende in Germania. L'implementazione precoce negli Stati Uniti, unita a minori vincoli di budget, può spiegare perché le aziende degli Stati Uniti sono più avanti nell'adozione della strategia Zero Trust rispetto alle aziende di altri mercati. Nello stesso modo, l'avvento relativamente recente della strategia Zero Trust in Germania permette di contestualizzare i tassi di adozione più bassi: il 97% delle aziende tedesche ha iniziato l'implementazione solo negli ultimi tre anni.

**Figura 5. Implementazione di Zero Trust**


| | USA (2020) | USA | DE | JP | AUS/NZ |
|---|---|---|---|---|---|
| Implementazione di Zero Trust | 70% | 79% | 75% | 76% | 71% |
| • Implementazione completa | 27% | 44% | 19% | 32% | 28% |
| • Implementazione in corso | 43% | 35% | 56% | 44% | 43% |

35% Implementazione completa

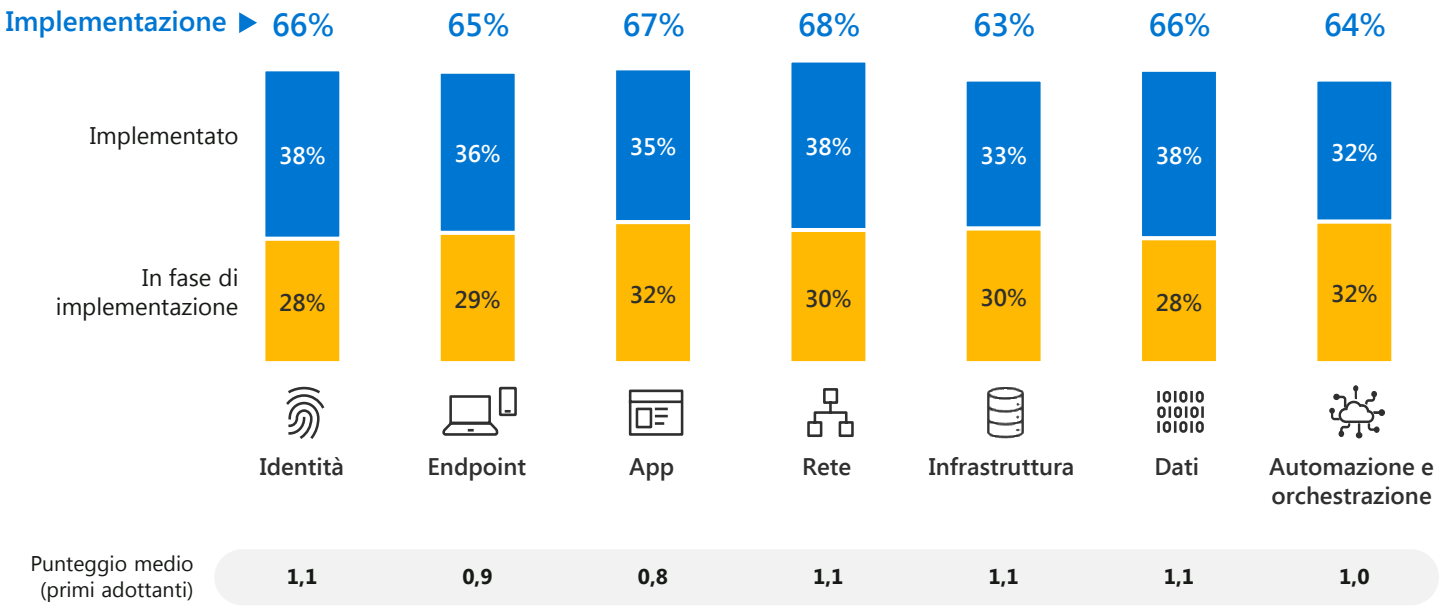
42% Implementazione in corso

# Non esiste un approccio unico all'implementazione di Zero Trust che permetta di avviarla in qualsiasi area

Nessun'area a rischio sicurezza (identità, endpoint, app, rete, infrastruttura, dati, automazione e orchestrazione) si distingue come punto di partenza principale della strategia Zero Trust perché meno del 15% delle aziende inizia dalla stessa area a rischio sicurezza. Le aziende stanno cominciando l'implementazione in aree diverse, probabilmente in base alle proprie esigenze e risorse interne disponibili. Alla fine, cercano di adottare la strategia Zero Trust in tutte le area a rischio sicurezza per garantire una protezione ancora maggiore contro le minacce, quindi la strategia Zero Trust viene percepita come una strategia end-to-end da completare nel corso del tempo (Figura 6).

Oltre alle aree a rischio sicurezza incluse nella strategia Zero Trust, le aziende devono identificare i singoli componenti di ogni area a rischio sicurezza a cui dare priorità. Per endpoint, app, rete, dati e automazione/orchestrazione non esiste un punto di partenza chiaro; i professionisti della sicurezza hanno opinioni disparate riguardo ai componenti da considerare assolutamente prioritari. In ogni caso, l'autenticazione avanzata viene in genere implementata prima per le identità, mentre gli strumenti di rilevamento delle minacce sono una priorità chiara in ambito infrastruttura (Figura 7).

**Figura 6. Implementazione dell'attuale modello Zero Trust: aree a rischio sicurezza**



## Figura 7. Prime 3 aree di implementazione del componente Zero Trust - 1° posto (adottata per prima)

| Identità | |
|---|---|
| Autenticazione avanzata (autenticazione a più fattori, autenticazione senza password) | 32% |
| Rilevamento dei rischi e azioni correttive automatici | 27% |
| Criteri di accesso adattivo per bloccare l'accesso alle risorse | 22% |

| App | |
|---|---|
| Shadow IT Discovery e valutazione dei rischi continue | 23% |
| Controllo granulare degli accessi alle app (es. visibilità limitata o sola lettura) | 22% |
| Controllo degli accessi basato su criteri per le app | 20% |

| Infrastruttura | |
|---|---|
| Accesso del team della sicurezza agli strumenti di rilevamento delle minacce | 25% |
| Protezione dei workload nel cloud (ambiente ibrido e multi-cloud) | 19% |
| Visibilità granulare e controllo degli accessi per tutti i workload (macchine virtuali, server, ecc.) | 17% |

| Automazione e orchestrazione | |
|---|---|
| Raggiungimento di una visibilità completa grazie a una piattaforma centralizzata per indagine e reazioni | 29% |
| Raccolta e analisi dei dati sulle minacce in vari domini (identità, endpoint, app, rete, infrastruttura) | 28% |
| Abilitazione di indagine e reazioni automatizzate | 22% |

| Endpoint | |
|---|---|
| Criteri/controlli per prevenire la perdita di dati per tutti i dispositivi non gestiti e gestiti | 27% |
| Valutazione dei rischi dei dispositivi in tempo reale/rilevamento delle minacce endpoint | 26% |
| I dispositivi sono registrati presso il provider di identità | 24% |

| Rete | |
|---|---|
| Controlli di accesso sicuri per proteggere le reti | 25% |
| Protezione dalle minacce e filtri con segnali basati sul contesto | 24% |
| Tutto il traffico è crittografato | 20% |

| Dati | |
|---|---|
| Le decisioni di accesso sono regolate dal motore dei criteri di sicurezza | 21% |
| I dati sono classificati ed etichettati | 21% |
| I file più sensibili sono sempre protetti con la crittografia | 20% |

> Non la consideravamo un semplice assieme di tecnologie, ma una strategia e un approccio per trattare ogni risorsa utente, all'interno o all'esterno della nostra rete, come non attendibile fino a quando non verificata.

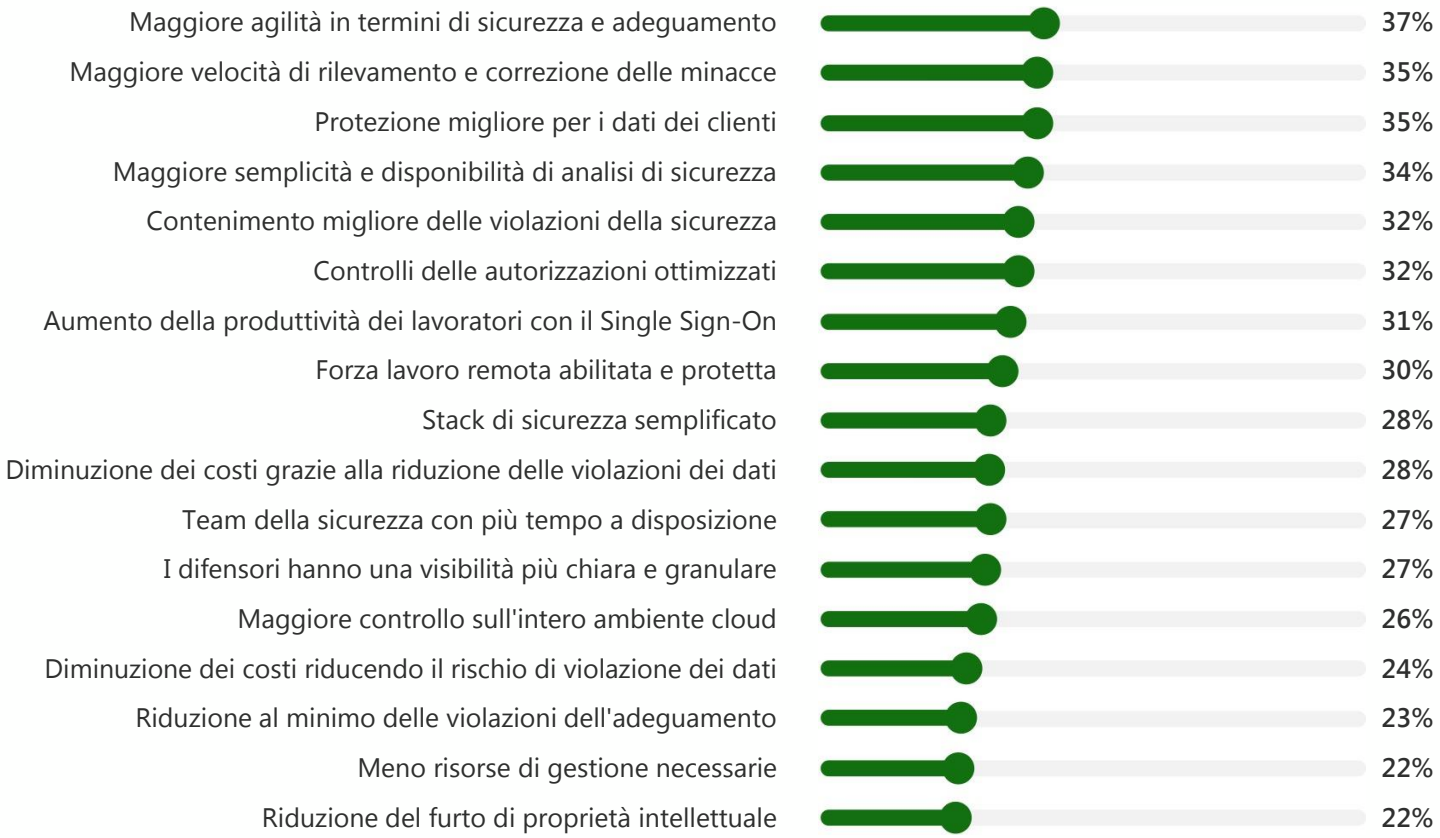
Decisore statunitense per la sicurezza
Ospitalità

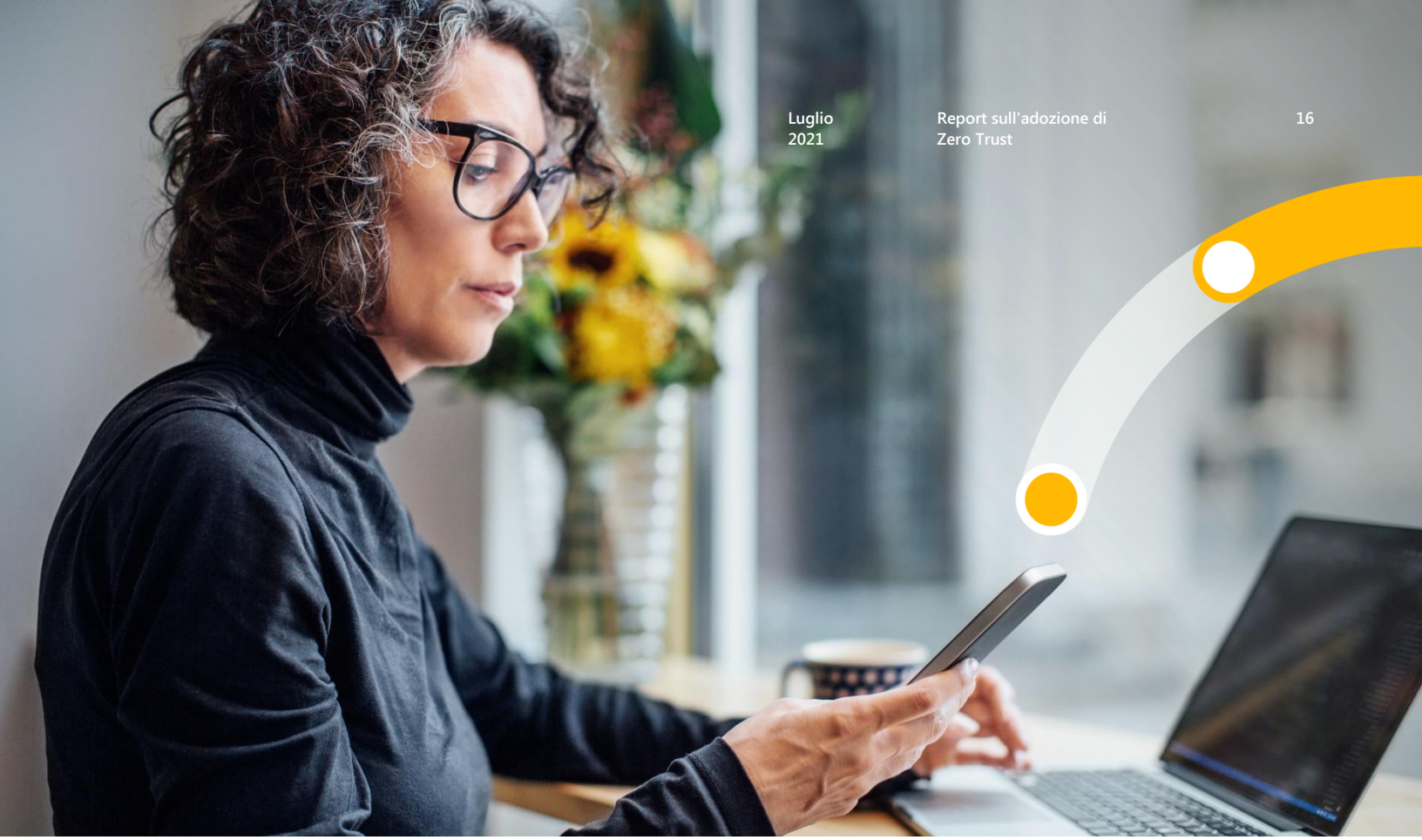
## Una volta che le aziende iniziano a implementare la strategia Zero Trust, i principali vantaggi includono una maggiore agilità, velocità e protezione; i vantaggi in termini di risorse sono meno comuni

Una volta implementata la strategia Zero Trust, le aziende beneficiano di una maggiore agilità (37%), velocità (35%) e protezione dei dati dei clienti (35%) (Figura 8). Tuttavia, sono meno frequenti i vantaggi diretti per i dipendenti, come un maggiore tempo a disposizione per il team della sicurezza (27%) e la riduzione del numero di risorse necessarie per la gestione dell'infrastruttura (22%).

Ecco un dato da sottolineare: le aziende ritengono che la strategia Zero Trust le aiuterà a gestire la maggior parte delle minacce e dei cambiamenti dell'ambiente, soprattutto per quanto riguarda la sicurezza IoT e OT (47%).

**Figura 8. Vantaggi di Zero Trust**





## Le aziende sono sicure di poter trarre il massimo vantaggio dalla strategia Zero Trust

Il 79% ha fiducia nella propria capacità di gestire le minacce alla sicurezza in genere, ma questa fiducia diminuisce quando la minaccia comporta la fabbricazione della realtà: i decisori per la sicurezza si sentono meno fiduciosi quando si tratta di gestire minacce che implicano identità sintetiche (20%) e deepfake (10%).

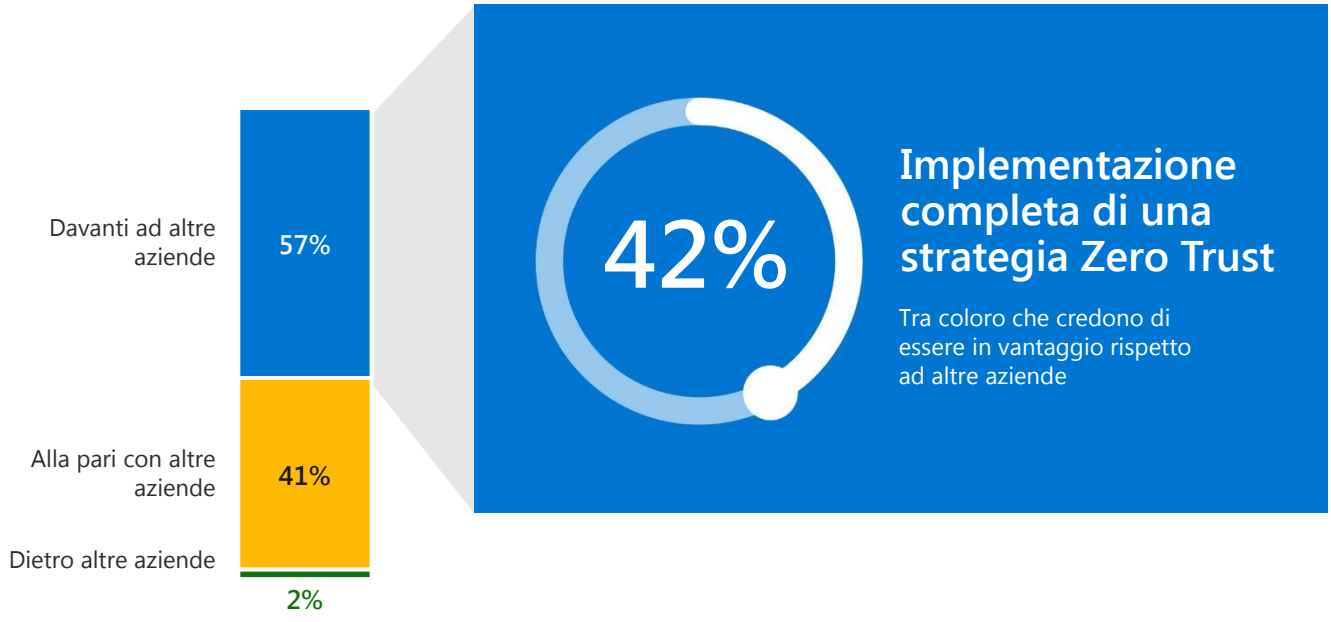
Alla luce dei vantaggi ottenuti, la strategia Zero Trust di solito genera associazioni positive. In tutti e quattro i mercati, i decisori per la sicurezza considerano l'approccio delle rispettive aziende pratico e ambizioso nello stesso tempo, descrivendolo come fiducioso (37%) ed efficiente (31%), ma anche come motivante (25%), stimolante (25%) e interessante (25). In Giappone, in particolare, i professionisti della sicurezza ritengono che il modello Zero Trust sia impegnativo (27%) e comporti una trasformazione radicale (25%), suggerendo che, nonostante le difficoltà di implementazione, i suoi vantaggi siano di vasta portata una volta avvenuta l'adozione.

# Tante aziende ritengono di essere a buon punto con l'implementazione di Zero Trust, ma devono lavorare ancora molto

Mentre solo il 35% delle aziende ha implementato completamente la strategia Zero Trust, il 52% afferma di essere in anticipo rispetto alle previsioni e il 57% ritiene di essere in anticipo rispetto ad altre aziende. Le aziende si considerano particolarmente a buon punto rispetto ad altre in Giappone (66%) e in Australia/Nuova Zelanda (63%). Mentre la fiducia abbonda in tutti i mercati, sembra esserci un divario tra percezione e realtà: tra coloro che ritengono di essere in anticipo rispetto ad altre aziende, solo il 42% dichiara di aver implementato completamente una strategia Zero Trust (vedi la Figura 9).

Anche se molte aziende hanno fiducia nella propria strategia Zero Trust e si sentono in grado di gestire future minacce alla sicurezza, c'è ancora molto da fare per realizzare l'implementazione completa in tutte le aree a rischio. Tra le aziende che ritengono di avere implementato completamente la strategia Zero Trust, ad esempio, quasi la metà non ha incluso alcune aree a rischio sicurezza, in particolare gli ambiti infrastruttura e identità.

**Figura 9. Confronto con l'implementazione di Zero Trust**




| | Stati Uniti | DE | JP | AUS/NZ |
|---|---|---|---|---|
| In anticipo | 59% | 46% | 66% | 63% |
| Alla pari | 40% | 52% | 34% | 32% |
| In ritardo | 2% | 2% | 0% | 6% |

# Guardando ai prossimi due anni, la strategia Zero Trust rimarrà una priorità assoluta per la sicurezza

Le aziende sono tutte a favore della strategia Zero Trust e i decisori sostengono che essa continuerà a essere la massima priorità per la sicurezza nei prossimi due anni. L'importanza relativa della strategia Zero Trust come iniziativa per la sicurezza dovrebbe aumentare (dal 53% al 58%) entro il 2023 perché i decisori per la sicurezza prevedono che tale strategia rimarrà fondamentale per il successo in genere (96%) (vedi la Figura 10).

Le criticità previste sono particolarmente alte tra le aziende del Giappone, dove il 70% afferma che la strategia Zero Trust sarà fondamentale nei prossimi due anni rispetto a una media complessiva del 56%. Anche il budget della strategia Zero Trust dovrebbe crescere e il 73% delle aziende prevede di aumentare il budget. Questa cifra, però, è leggermente inferiore in Germania (67%), dove il 31% delle aziende prevede che il budget rimarrà invariato (vedi la Figura 11).

**Figura 10. Criticità previste per Zero Trust nei prossimi due anni**

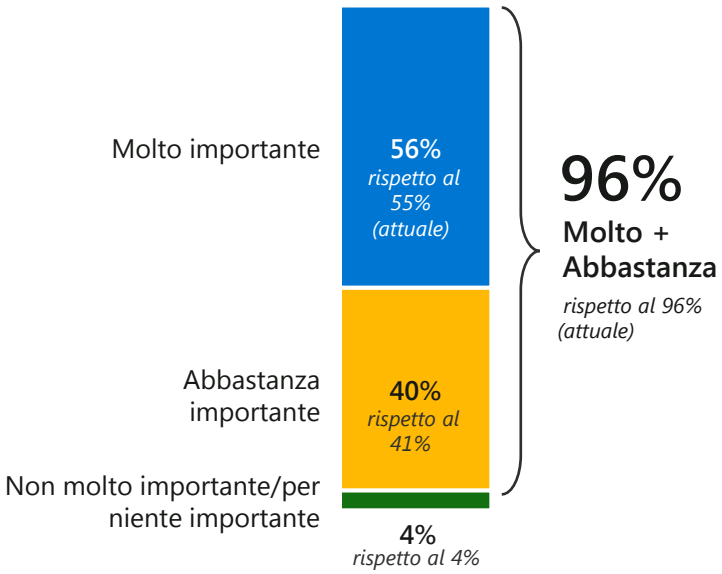
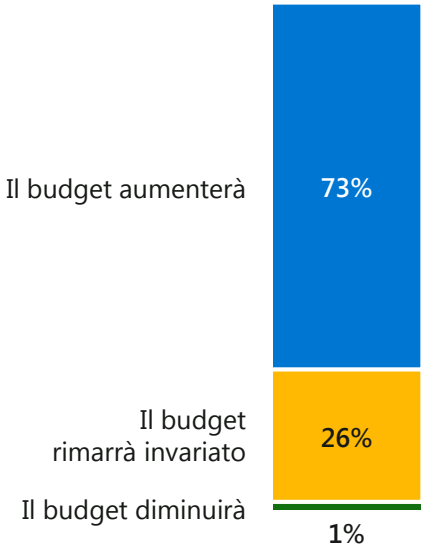
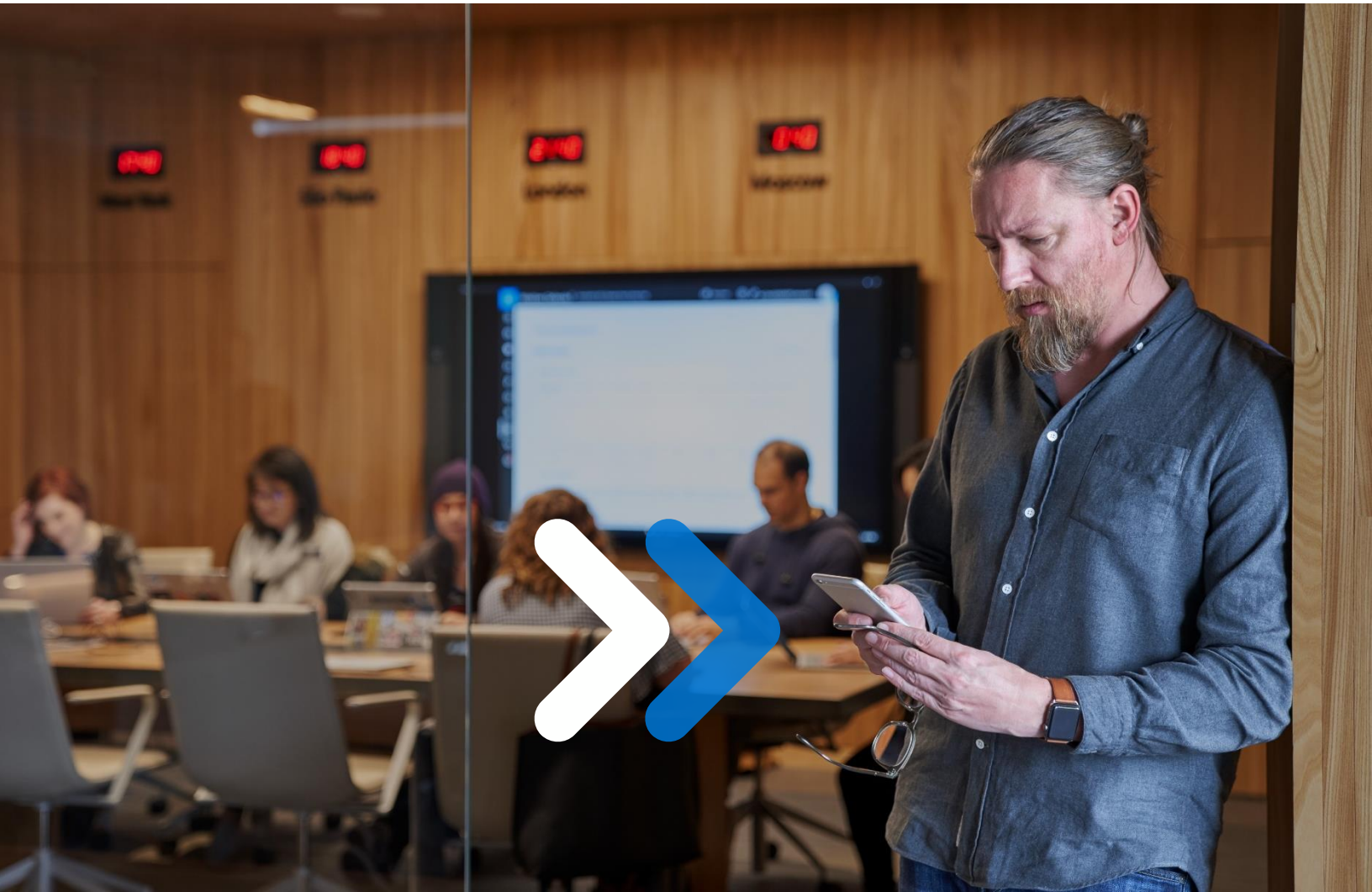



**Figura 11. Budget per Zero Trust previsto nei prossimi due anni**



## I successi comprovati della strategia Zero Trust potrebbero alimentare ulteriori investimenti

Le aziende che hanno aderito con slancio a Zero Trust prevedono di raddoppiare l'investimento nei prossimi due anni e quelle che non hanno ancora iniziato l'adozione rischiano di restano indietro. Queste aziende non solo sono indietro rispetto alle aziende concorrenti che hanno già completato l'implementazione in termini di priorità data a Zero Trust nei piani di sicurezza (42% rispetto al 66%) e di previsione di aumento del budget (66% rispetto al 72%), ma si sentono anche molto meno fiduciose in ambiti quali la gestione IoT e la sicurezza OT in futuro (40% rispetto al 53%).



# Superare le sfide dei dipendenti sarà un fattore chiave per raddoppiare l'investimento in Zero Trust

Nonostante i rapidi progressi nell'adozione della strategia Zero Trust, le aziende devono superare numerose sfide se vogliono progredire ulteriormente in termini di implementazione (Figura 12). Le sfide relative a risorse e leadership sono prevalenti in queste categorie. Il tempo necessario per implementare le strategie Zero Trust e la mancanza di supporto da parte dei massimi dirigenti sono i maggiori ostacoli e quest'ultimo è particolarmente rilevante in Australia/Nuova Zelanda (65%).

Anche i vincoli di bilancio, che il 45% delle aziende identificano come un ostacolo, probabilmente incidono nelle sfide relative alle risorse e alla leadership.

Il 21% dei decisori per la sicurezza, ad esempio, cita la difficoltà di dimostrare il ROI di un investimento nella strategia Zero Trust come un ostacolo all'implementazione: un problema che può portare alla mancanza di un consenso da parte dei massimi dirigenti. Poiché nei mercati non statunitensi sono più probabili i vincoli di budget (60% delle aziende in Giappone, 57% in Germania, 57% in Australia/Nuova Zelanda), è possibile che questo abbia un effetto a catena, portando a un'implementazione delle strategie Zero Trust più limitata e lenta in Giappone, Germania e Australia/Nuova Zelanda rispetto agli Stati Uniti.

**Figura 12. Ostacoli a Zero Trust**

| Problemi di risorse 60% | Leadership 53% | IT 46% | Fornitore 46% | Limiti di budget 45% |
|---|---|---|---|---|
| **20%:** l'implementazione richiede troppo tempo | **20%:** manca il supporto dei massimi dirigenti | **21%:** ci sono difficoltà a integrare le soluzioni di sicurezza | **21%:** occorre un supporto per l'implementazione da parte dei fornitori | **21%:** costo di implementazione di una strategia Zero Trust |
| **19%:** manca una gestione interna del cambiamento | **19%:** manca il supporto delle parti interessate | **19%:** vi è incompatibilità con i sistemi legacy | **21%:** vi sono difficoltà a identificare i fornitori adatti | **21%:** difficoltà a dimostrare il ROI |
| **18%:** occorrono più materiali di formazione | **19%:** occorre assistenza per creare un business case convincente | **19%:** vi sono difficoltà di scalabilità in tutta l'azienda | **17%:** impossibilità di trovare partner innovativi | **14%:** budget insufficiente |
| **17%:** non necessaria per un'azienda delle nostre dimensioni | **18%:** manca il consenso a livello di organizzazione | | | |
| **16%:** mancano i talenti per un'implementazione corretta | | | | |

"Ottenere il consenso iniziale è stato arduo, ma una volta d'accordo come parti interessate a investire in questo progetto, c'è stata adesione da parte di tutti".

Decisore statunitense per la sicurezza FinTech

## I decisori per la sicurezza hanno una leggera propensione per i fornitori generali o consolidati

In fatto di strategia dei fornitori Zero Trust, le aziende devono decidere tra l'approccio del fornitore unico e la soluzione più all'avanguardia. La prima strategia prevede l'acquisto di una suite di prodotti per l'intera architettura Zero Trust da un fornitore generale o consolidato: una soluzione che secondo i decisori per la sicurezza offre maggiori competenze, risorse e semplicità per le aziende con poche risorse interne. Tuttavia, i dubbi su approccio includono un aumento della vulnerabilità e la mancanza di flessibilità (vedi la Figura 13).

Per quest'ultima strategia all'avanguardia, occorre ottenere i singoli componenti tecnologici Zero Trust da fornitori specializzati. A differenza della soluzione del fornitore unico, questa strategia si basa su provider specializzati in aree diverse che offrono quindi una maggiore flessibilità e possono allinearsi meglio alla strategia dell'azienda. Detto questo, i professionisti della sicurezza considerano le soluzioni all'avanguardia più costose e impegnative in termini di risorse e ritengono che ostacolino la visibilità, tutti svantaggi che in definitiva comportano sfide per i fornitori e il budget (vedi la Figura 14).

Se le aziende sono in gran parte divise, una leggera maggioranza di decisori per la sicurezza (55%) preferisce lavorare con fornitori generali (fornitore unico). Le aziende di Australia/Nuova Zelanda, tuttavia, si muovono tendenzialmente nella direzione opposta e il 52% di esse preferisce le soluzioni più all'avanguardia.

**Figura 13. Vantaggi del fornitore unico e ostacoli (primi 2)**

| ⊕ Vantaggi del fornitore unico | |
|---|---|
| Il fornitore dispone di competenze specifiche del settore per tutte le soluzioni | 24% |
| Più risorse disponibili per pianificare una strategia Zero Trust | 23% |
| Stack di sicurezza semplificato | 22% |

| ⊖ Svantaggi del fornitore unico | |
|---|---|
| Fare affidamento su un solo fornitore aumenta la vulnerabilità | 34% |
| Comporta un'integrazione più complessa con l'architettura legacy | 33% |
| Meno flessibilità per funzionalità specifiche | 29% |

**Figura 14. Vantaggi delle soluzioni all'avanguardia e ostacoli (primi 2)**

| ⊕ Vantaggi della soluzione più all'avanguardia | |
|---|---|
| Flessibilità per perseguire le soluzioni migliori per qualsiasi componente della strategia Zero Trust | 33% |
| Allineamento migliore della soluzione con l'architettura o la strategia dell'azienda | 30% |
| Maggiori opportunità di innovazione grazie a vari fornitori | 26% |

| ⊖ Svantaggi della soluzione più all'avanguardia | |
|---|---|
| Aumento dei costi | 29% |
| Impossibilità di condividere i dati tra diverse soluzioni | 26% |
| Numero elevato di soluzioni che i team interni dovranno adottare e gestire | 26% |

# Conclusioni

Poiché i rischi per la sicurezza diventano non solo più frequenti, ma anche più nefasti, le aziende di tutti i mercati e di tutti i settori optano per una strategia Zero Trust che le guidi a "non fidarsi mai, verificare sempre". La strategia Zero Trust è la massima priorità per la sicurezza delle aziende che mirano ad aumentare il livello generale di sicurezza e la produttività, a migliorare l'esperienza degli utenti finali, a semplificare le procedure di sicurezza per i dipendenti e a ridurre i costi. Tuttavia, se tutti sono concordi sui vantaggi di una strategia Zero Trust, le risorse limitate e lo scetticismo della leadership ne ostacolano un'implementazione universale.

L'adozione della strategia Zero Trust ha subito un'accelerazione negli ultimi tre anni, in parte a causa della pandemia di COVID-19. Fondamentalmente, il passaggio ad ambienti di lavoro remoti e ibridi sta promuovendo una più ampia adozione degli approcci Zero Trust, che promettono di salvaguardare sistemi e dati anche quando i dipendenti accedono ad essi quando si trovano fuori sede, a volte da dispositivi personali. L'adozione accelerata dal COVID fa presumere una generale preparazione a Zero Trust e le aziende che hanno adottato questa strategia durante la pandemia ne hanno eseguito l'implementazione in aree a rischio sicurezza più numerose rispetto alle altre aziende.

Detto questo, anche gli adottanti più avanzati della strategia Zero Trust devono lavorare ancora molto e le idee sbagliate delle aziende sulla propria maturità Zero Trust potrebbero lasciare alcune vulnerabilità di cui queste aziende non sono neppure consapevoli.

La maggior parte delle aziende in tutti i mercati ritiene che l'importanza di una strategia Zero Trust non farà altro che aumenterà con il tempo e prevede un conseguente aumento del budget. Il cambiamento previsto in termini di priorità è particolarmente cruciale per i mercati non statunitensi, dove le preoccupazioni legate al budget costituiscono ostacoli rilevanti all'adozione. L'impegno per una implementazione completa può essere gravoso dal punto di vista finanziario e logistico; eppure, i vantaggi di un approccio Zero Trust sono innegabili e Microsoft è pronta a guidare e supportare le aziende che intraprendono questo promettente percorso.

Per saperne di più su Zero Trust e valutare la maturità Zero Trust della tua azienda, visita

**aka.ms/zerotrust**

# Obiettivi di ricerca dettagliati e selezione dei destinatari

Alcuni obiettivi della ricerca:

Comprendere lo stato attuale degli approcci Zero Trust

Scoprire atteggiamenti, procedure consigliate, vantaggi e sfide dell'adozione degli approcci Zero Trust

Esplorare il futuro degli approcci Zero Trust

Contestualizzare le innovazioni e le tendenze degli approcci Zero Trust

Per soddisfare i criteri di selezione, i decisori per la sicurezza dovevano essere:

Responsabili della sicurezza all'interno dell'azienda (sicurezza informatica, operazioni di sicurezza, protezione dalle minacce, gestione delle identità, gestione dei rischi, sicurezza delle applicazioni, analisi forensi digitali e risposta agli incidenti, ecc.)

Impiegati a tempo pieno in una grande azienda (oltre 1.000 dipendenti negli Stati Uniti; oltre 500 dipendenti in Germania, Giappone, Australia e Nuova Zelanda)

Età 25-75

Familiarità con Zero Trust

Coinvolti nel processo decisionale per lo sviluppo/l'implementazione di una strategia Zero Trust

Dei 911 decisori per la sicurezza intervistati per la sessione di ricerca di aprile 2021:

Negli Stati Uniti sono stati intervistati 477 decisori

In Germania sono stati intervistati 201 decisori

In Australia/Nuova Zelanda sono stati intervistati 126 decisori

In Giappone sono stati intervistati 107 decisori

*Nota: la ricerca è stata condotta durante la pandemia globale di COVID-19 in varie fasi di intensificazione/contenimento*



Microsoft Security hypothesis