La trasformazione zero trust nel 2023

DALLA PREVENZIONE ALL'ABILITAZIONE:
sfruttare il pieno potenziale dello zero trust per supportare le aziende altamente mobili e incentrate sul cloud

Contenuti

Riepilogo

Nathan Howe | Vice President, Emerging Technology & 5G, Zscaler

Nel periodo della trasformazione digitale rapida, lo zero trust si è contraddistinto come il framework ideale per proteggere utenti, carichi di lavoro e dispositivi aziendali in un mondo cloud altamente distribuito e incentrato sulla mobilità.

I responsabili dell'IT a livello globale se ne sono resi conto, e l'approccio zero trust si è diffuso, rivoluzionando decenni di pratiche di sicurezza e di rete.

Oltre il 90% dei responsabili IT che hanno avviato la migrazione verso il cloud ha implementato o implementerà una strategia di sicurezza fondata sullo zero trust nel corso del prossimo anno.

Questo è quanto emerge dalla nostra ultima indagine globale, che ha raccolto le opinioni di oltre 1900 CIO, CISO, CDO, CTO e responsabili delle infrastrutture attivi in organizzazioni che hanno già iniziato a spostare le applicazioni e i servizi sul cloud.

Si tratta di un progresso importante motivato da un ottimismo a supporto dell'implementazione dell'architettura zero trust che si estende anche oltre i prossimi 12 mesi.

22%

I risultati indicano che solamente il 22% è pienamente convinto che la propria organizzazione stia sfruttando appieno il potenziale dell'infrastruttura cloud; questo significa che in futuro, le aziende non dovranno pensare solo alla sicurezza.

I percorsi di adozione del cloud proseguono, e l'utilizzo dello zero trust per migliorare la sicurezza è ormai chiaro. Oltre due terzi (68%) dei responsabili IT concordano sul fatto che la trasformazione sicura del cloud è impossibile con un'infrastruttura di sicurezza della rete legacy, o che lo ZTNA presenta dei chiari vantaggi rispetto ai firewall e alle VPN tradizionali per la protezione dell'accesso remoto alle applicazioni.

I risultati indicano che solamente il 22% è pienamente convinto che la propria organizzazione stia sfruttando appieno il potenziale dell'infrastruttura cloud; questo significa che in futuro, le aziende non dovranno pensare solo alla sicurezza. Da una prospettiva IT olistica, lo zero trust ha il potenziale per sbloccare un'infinità di opportunità in un processo di digitalizzazione generale; sì, è sicuramente in grado di prevenire gli attacchi informatici su larga scala, ma può fare anche molto di più: favorire una maggiore innovazione, migliorare il coinvolgimento dei dipendenti o fornire efficienze tangibili in termini di costi.

Le organizzazioni stanno adottando ambienti di lavoro moderni, flessibili e basati su una moltitudine di tecnologie emergenti, come IoT/OT, 5G e perfino il metaverso, e per questo motivo devono iniziare a pensare allo zero trust e alla trasformazione digitale in modo più ampio. Una piattaforma zero trust ha il potere di ridisegnare i requisiti dell'infrastruttura aziendale e organizzativa, e può diventare un vero e proprio fattore abilitante per il business, consentendo alle aziende di supportare il modello di lavoro flessibile richiesto dai dipendenti, ma anche di diventare delle organizzazioni completamente digitalizzate, con tutti i vantaggi che ne derivano: agilità, efficienza e un'infrastruttura a prova di futuro.

Abbiamo commissionato questa ricerca per scoprire la situazione della trasformazione zero trust all'interno delle organizzazioni. Quello che abbiamo scoperto è promettente: i tassi di implementazione sono elevati, ma le motivazioni potrebbero essere più ambiziose. I responsabili IT hanno nelle loro mani l'incredibile opportunità di fornire ai responsabili delle decisioni aziendali le informazioni giuste sullo zero trust, e di proporre quest'ultimo come un motore per l'azienda: è l'anello mancante che aiuta le aziende a responsabilizzarsi e prepararsi sin da subito ad adottare le tecnologie del futuro.

ULTIMI DATI SULLO ZERO TRUST

90% Oltre il 90% delle organizzazioni che hanno iniziato la migrazione sul cloud ha implementato o implementerà una strategia di sicurezza zero trust nei prossimi 12 mesi

88% A livello globale, l'88% dei responsabili IT crede che la propria organizzazione stia sfruttando il potenziale dell'infrastruttura cloud, ma solo il 22% ne è pienamente convinto

A LIVELLO REGIONALE, LA PERCENTUALE DI INTERVISTATI CHE SI DICHIARANO PIENAMENTE CONVINTI DI SFRUTTARE IL PIENO POTENZIALE DELL'INFRASTRUTTURA CLOUD È:

N° 1 Lo ZTNA è l'investimento di tecnologia zero trust con la maggiore priorità nei prossimi 12 mesi; questo indica l'importanza dell'accesso remoto nell'ambiente di lavoro flessibile

68% Oltre due terzi (68%) dei responsabili IT credono che la trasformazione sicura del cloud sia impossibile con un'infrastruttura di sicurezza di rete legacy, oppure che lo ZTNA (Zero Trust Network Access) presenti dei chiari vantaggi rispetto ai firewall e alle VPN tradizionali per la protezione dell'accesso remoto alle applicazioni

54% dei responsabili IT ha dichiarato di ritenere che le VPN o i firewall perimetrali siano entrambi inefficaci per proteggere dagli attacchi informatici o fornire la visibilità sul traffico delle applicazioni e sugli attacchi

I PRINCIPALI OSTACOLI ALLA REALIZZAZIONE DEL PIENO POTENZIALE DEL CLOUD:

45% Le sfide della sicurezza dei dati sul cloud e i problemi di privacy

42% Complessità della rete e hardware di sicurezza difficile da scalare

40% Accesso remoto e di terze parti a IoT e OT

33% Connettività non uniforme e scarsa esperienza di accesso remoto per gli utenti

OLTRE A SICUREZZA, ACCESSO E COMPLESSITÀ, I PRINCIPALI MOTIVI A SUPPORTO DELL'IMPLEMENTAZIONE DI UN'ARCHITETTURA ZERO TRUST NON COSTITUISCONO ASPETTI STRATEGICI:

65% Miglioramento del rilevamento delle minacce avanzate o degli attacchi alle applicazioni web e incremento della sicurezza dei dati sensibili

44% Protezione dell'accesso remoto per fornitori, partner e tecnologia operativa

27% Potenziamento della connettività sicura per la forza lavoro flessibile

24% Riduzione della complessità e dei costi della sicurezza di rete legacy

Sezione I

Lo zero trust nel contesto del cloud

In questa indagine, quando facciamo riferimento al "cloud", parliamo di applicazioni, dati e carichi di lavoro forniti come servizi ospitati tramite la rete Internet, e non attraverso un data center locale all'interno di una rete aziendale. Alcuni esempi: SaaS (Software as a Service), IaaS (Infrastructure as a Service), PaaS (Platform as a Service) o applicazioni private sviluppate o ospitate sul cloud.

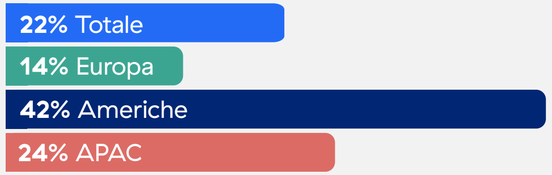
Prima di approfondire il concetto di zero trust, definiremo il contesto della sua adozione, per comprendere ciò che accade nel panorama IT che lo circonda e soprattutto a che punto sono le organizzazioni con i loro percorsi di adozione del cloud.

Gli eventi degli ultimi anni hanno sicuramente accelerato il passaggio al cloud. In molte organizzazioni, il processo è già in corso, se non si è già addirittura concluso.

Abbiamo intervistato oltre 1900 CIO, CISO, CDO, CTO e responsabili delle infrastrutture di tutto il mondo attivi in organizzazioni che hanno già iniziato a spostare le applicazioni e i servizi sul cloud. Di essi, quasi la metà (46%) ha dichiarato che il processo di migrazione è stato completato al 100%.

Tuttavia, sebbene l'88% dei responsabili IT ritenga che l'organizzazione stia sfruttando al meglio il proprio percorso verso il cloud, solo il 22% è pienamente convinto che la propria organizzazione stia ottenendo il massimo dall'infrastruttura cloud.

INTERVISTATI CONVINTI CHE L'ORGANIZZAZIONE STIA ATTUALMENTE SFRUTTANDO IL PIENO POTENZIALE DELL'INFRASTRUTTURA CLOUD



% DEGLI INTERVISTATI CHE SI DICHIARANO CONVINTI DEL FATTO CHE LA PROPRIA ORGANIZZAZIONE STIA ATTUALMENTE SFRUTTANDO APPIENO IL POTENZIALE DELL'INFRASTRUTTURA CLOUD

Passa con il mouse sopra ai Paesi per ulteriori dettagli.

Europa:

- 9% Germania
- 11% Francia
- 11% Spagna
- 19% Regno Unito

Americhe:

- 41% USA
- 51% Brasile

APAC:

- 16% Singapore
- 55% India

Esaminando le differenze regionali si evince che i responsabili IT europei sono i più dubbiosi in merito all'utilizzo della propria infrastruttura cloud: solo il 14% esprime convinzione. Nelle Americhe, tuttavia, questa percentuale è del 42%.

Anche se alla base di questa disparità non vi è una motivazione univoca e definita, una possibile ragione potrebbe risiedere nelle differenze interculturali riguardo alla velocità di adozione di tecnologie innovative; l'Europa adotta infatti un approccio più attento e presta maggiore attenzione alla privacy dei dati. Inoltre, l'infrastruttura di connettività ben consolidata dell'Europa e la forte attenzione alla produzione estendono le tempistiche con cui i tradizionali processi aziendali cambiano, e non si avverte la necessità immediata di adottare innovazioni come il 5G. Come approfondiremo in una sezione successiva, le organizzazioni delle Americhe invece si concentrano maggiormente sulle tecnologie emergenti, come l'intelligenza artificiale, il machine learning e la realtà aumentata; questo suggerisce che abbiano già in atto dei piani per consentire all'infrastruttura cloud di supportare casi d'uso più sofisticati.

Ma vediamo più in generale perché le organizzazioni faticano a sfruttare appieno il potenziale del cloud.

La sicurezza sembra essere l'ostacolo principale, perché i responsabili IT hanno selezionato due risposte legate a questo aspetto per rispondere a questa domanda:

I PRINCIPALI OSTACOLI CHE IMPEDISCONO DI REALIZZARE IL PIENO POTENZIALE DEL CLOUD

45% Preoccupazioni relative alla privacy dei dati e sfide legate alla sicurezza dei dati sul cloud

42% La rete è molto complessa da adattare e la sicurezza della rete è difficile da scalare

40% Problemi ad abilitare l'accesso di terzi e l'accesso remoto ai sistemi IoT e OT

33% Connettività incoerente e scarsa esperienza di accesso remoto per gli utenti

I PRINCIPALI OSTACOLI CHE IMPEDISCONO DI REALIZZARE IL PIENO POTENZIALE DEL CLOUD PER PAESE

Passa con il mouse sopra ai Paesi per ulteriori dettagli.

In Europa e nell'APAC dominano le preoccupazioni legate alla privacy dei dati:

- 36% Spagna
- 34% India
- 33% Italia
- 32% Australia
- 28% Francia

Nelle Americhe, le organizzazioni faticano ad affrontare le sfide legate alla protezione dei dati sul cloud:

- 44% Brasile
- 30% USA

al contempo, Singapore e il Giappone, in particolare, faticano ad adattare le prestazioni dell'hardware alla sicurezza della rete:

- 41% Singapore
- 30% Giappone

In un ambiente cloud, la superficie di attacco si estende in modo esponenziale: ogni servizio, utente e dispositivo che si interfaccia con Internet diventa una potenziale porta di ingresso vulnerabile che deve essere protetta dalle minacce.

E le organizzazioni hanno dei buoni motivi per essere preoccupate. In un ambiente cloud, la superficie di attacco si estende in modo esponenziale: ogni servizio, utente e dispositivo che si interfaccia con Internet diventa una potenziale porta di ingresso vulnerabile che deve essere protetta dalle minacce. Illustreremo meglio questo aspetto nella prossima sezione.

Ma se si osservano le principali motivazioni a supporto delle migrazioni sul cloud, è evidente che i responsabili IT vedono il cloud in modi diversi, e questo senza dubbio ne influenza l'uso effettivo. Alla domanda sui principali fattori alla base dei progetti di trasformazione digitale nelle loro organizzazioni, tre aspetti sono risultati in testa: la riduzione dei costi, la facilitazione dell'innovazione tecnologica e la gestione del rischio informatico.

I PRINCIPALI FATTORI CHE MOTIVANO I PROGETTI DI TRASFORMAZIONE DIGITALE SECONDO I RESPONSABILI IT GLOBALI SONO:

- Riduzione **dei costi** dell'infrastruttura IT
- Supporto di innovazioni **come il 5G e l'edge computing**
- Mitigazione **dei rischi per la sicurezza** informatica
- Gestione **degli ambienti multicloud**
- Miglioramento della capacità di attrarre e trattenere **i professionisti**

I PRINCIPALI FATTORI CHE MOTIVANO I PROGETTI DI TRASFORMAZIONE DIGITALE PER PAESE

Passa con il mouse sui Paesi per vedere maggiori dettagli.

Il Brasile si allinea al pensiero della maggioranza globale: la maggior parte delle organizzazioni indica la riduzione dei costi dell'infrastruttura IT come fattore principale.

In alcuni Paesi europei, tuttavia, la situazione è ben diversa. In Francia, le organizzazioni sono maggiormente interessate a favorire il lavoro flessibile, mentre per la Svezia la principale priorità è l'esperienza utente.

Il supporto di innovazioni come il 5G e l'edge computing risulta più importante nei Paesi che guardano più al futuro, come Giappone, Messico e Singapore. Altrettanto importante a Singapore è la crescita del fatturato.

L'ottimizzazione dei processi aziendali è invece uno dei tre fattori principali per Brasile e Spagna.

Tutti questi fattori sono molto pratici e guidati dall'IT. In realtà, l'elevata importanza della riduzione dei costi, seppur comprensibile nel clima attuale, indica che potrebbe esserci ancora una mancanza di comprensione riguardo ai principali vantaggi offerti dal cloud. E questo, a sua volta, potrebbe avere un impatto sull'approccio e sull'utilizzo delle tecnologie utilizzate a suo supporto, **come lo zero trust.**

Gli eventi degli ultimi anni hanno sicuramente accelerato il passaggio al cloud.

Sezione II

Supportare l'uso dello zero trust

Lo zero trust è un approccio olistico alla protezione delle organizzazioni moderne, basato sull'accesso a privilegi minimi e sul principio che nessun utente o applicazione sia intrinsecamente attendibile. Si fonda sull'ipotesi che tutto sia ostile, e stabilisce l'attendibilità solo in base all'identità e al contesto dell'utente, con policy per il controllo dell'accesso in ogni fase del percorso. Secondo il National Institute of Standards and Technology (NIST) statunitense, il principio fondante di un'architettura zero trust consiste nel fatto che l'attendibilità non deve essere concessa in modo implicito alle risorse o agli account utente esclusivamente sulla base della loro ubicazione fisica o di rete (ad esempio, reti LAN rispetto a Internet) o sulla titolarità delle risorse (aziendali o personali). In poche parole, prima di fidarsi, è sempre meglio verificare.

In cima alle preoccupazioni dei responsabili IT ci sono i problemi della sicurezza, del controllo degli accessi e della complessità; per questo motivo, non sorprende che molte organizzazioni si interessino allo zero trust per superare questi ostacoli. Le risposte dimostrano che le organizzazioni stanno acquisendo una buona conoscenza di base dei vantaggi per la sicurezza offerti dallo zero trust in questo nuovo ambiente operativo, rispetto agli approcci più tradizionali.

Alle domande riguardo all'infrastruttura di rete e sicurezza legacy, il 54% dei responsabili IT ha dichiarato di ritenere le VPN o i firewall perimetrali inefficaci per proteggere contro gli attacchi informatici o fornire visibilità sul traffico delle applicazioni e gli attacchi. Un altro 68% ha riconosciuto che, per quanto riguarda la protezione dell'accesso remoto alle applicazioni, lo ZTNA (Zero Trust Network Access) presenta dei chiari vantaggi rispetto ai firewall e alle VPN tradizionali, oppure che la trasformazione cloud sicura non può essere raggiunta con le tradizionali infrastrutture di sicurezza della rete.

Passa con il mouse sui Paesi per vedere maggiori dettagli.

Gli intervistati che concordano sull'impossibilità di ottenere una trasformazione cloud sicura con un'infrastruttura di sicurezza di rete legacy e sui chiari vantaggi offerti dallo ZTNA rispetto ai firewall e alle VPN tradizionali per la protezione dell'accesso remoto alle applicazioni

- 85% India
- 81% USA
- 75% Brasile
- 75% Singapore
- 73% Svezia

Gli intervistati che concordano sull'inefficacia di VPN e firewall perimetrali per la protezione dagli attacchi informatici o per fornire visibilità sul traffico delle applicazioni e sugli attacchi:

- 72% India
- 65% Singapore
- 64% Giappone
- 57% Germania
- 56% USA

Gli intervistati che concordano sulla necessità di strumenti integrati per l'analisi, la risoluzione dei problemi e la correzione dei problemi dell'esperienza utente per i team di IT (oltre alla sicurezza):

- 70% India
- 63% Messico
- 62% USA
- 56% Singapore
- 51% Spagna
- 50% Giappone

90%

Oltre il 90% degli intervistati che hanno iniziato la migrazione sul cloud ha implementato o implementerà una strategia di sicurezza zero trust nei prossimi 12 mesi.

Oltre a questa consapevolezza, la cosa più promettente è che le aziende stanno agendo di conseguenza. Oltre il 90% degli intervistati che hanno iniziato la migrazione sul cloud ha implementato o implementerà una strategia di sicurezza zero trust nei prossimi 12 mesi.

L'Italia e l'India fanno da apripista per quanto concerne l'attuazione di una strategia zero trust, con il 97% delle organizzazioni italiane e il 96% di quelle indiane che confermano di averla già implementata o di averla in programma.

Passa con il mouse sui Paesi per vedere maggiori dettagli.

La percentuale di organizzazioni che hanno già adottato una strategia di sicurezza zero trust, che la stanno attualmente implementando o che la stanno pianificando:

- 97% Italia
- 96% India
- 95% Regno Unito
- 95% USA
- 94% Giappone
- 93% Brasile
- 93% Singapore
- 92% Germania
- 91% Messico
- 90% Paesi Bassi
- 89% Spagna
- 89% Francia
- 88% Australia
- 85% Svezia

Lo zero trust viene ancora visto prevalentemente come una soluzione (di sicurezza) che riguarda solo il reparto IT, ma può offrire molto di più alle organizzazioni.

Purtroppo però, avere adottato un sistema di sicurezza zero trust o averne in programma l'implementazione, non indica che si stia sfruttando tutto il suo potenziale di fattore abilitante per il business.

In realtà, i risultati indicano che lo zero trust viene ancora visto prevalentemente come una soluzione (di sicurezza) che riguarda solo il reparto IT. Questo, a sua volta, significa che viene impiegato unicamente per risolvere i problemi di sicurezza e ottenere benefici tattici, quando invece può offrire molto di più alle organizzazioni.

I PRINCIPALI MOTIVI PER IMPLEMENTARE UN'ARCHITETTURA ZERO TRUST

65% Miglioramento del rilevamento delle minacce avanzate o degli attacchi alle applicazioni web e incremento della sicurezza dei dati sensibili

44% Protezione dell'accesso remoto per fornitori, partner e tecnologia operativa

27% Potenziamento della connettività sicura per la forza lavoro flessibile

24% Riduzione della complessità e dei costi di sicurezza della rete legacy

IL PRINCIPALE MOTIVO PER IMPLEMENTARE UN'ARCHITETTURA ZERO TRUST NELLE VARIE PARTI DEL MONDO:

Passa con il mouse sui Paesi per vedere maggiori dettagli.

Per migliorare la rilevazione delle minacce avanzate:

- 52% India
- 42% Singapore
- 41% USA
- 39% Italia
- 36% Spagna
- 30% Francia
- 26% Regno Unito

Per migliorare il rilevamento degli attacchi alle applicazioni web:

- 44% Brasile
- 35% Messico

Per incrementare la sicurezza e proteggere i dati sensibili:

- 44% Brasile

Per fornire un accesso remoto sicuro a fornitori, partner e collaboratori:

- 33% Australia
- 32% Giappone
- 24% Paesi Bassi

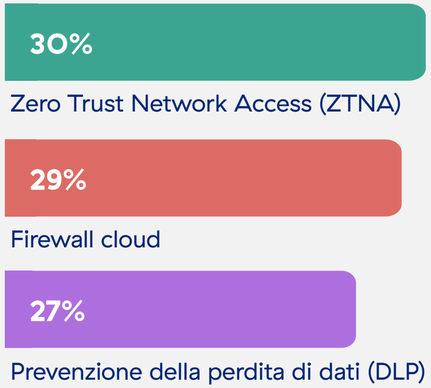
L'utilizzo dello zero trust per scopi di sicurezza e solo all'inizio del percorso di trasformazione ne limita significativamente il potenziale, in particolare in un momento in cui il successo di un'organizzazione dipende molto dalla sua capacità di digitalizzarsi e innovarsi, rapidamente e su larga scala.

Comprendendolo più a fondo, e non considerandolo solo come una tecnologia o un prodotto, può consentire alle aziende di semplificare la propria infrastruttura, di ripensare il modo in cui operano e di trasformarsi in realtà completamente digitalizzate. Ad esempio, le aziende che hanno adottato lo zero trust dispongono di un inventario completo e accurato di tutte le loro applicazioni e di tutto ciò che è presente all'interno dell'organizzazione. Sulla base di questo inventario, sono in grado di prendere decisioni strategiche su come ottimizzare i processi, ridurre i costi, eliminare l'hardware legacy e migliorare l'efficienza.

Tuttavia, per ottenere tutti questi vantaggi strategici, le organizzazioni devono essere in grado di comunicare il potenziale dello zero trust al consiglio di amministrazione, in modo che questo approccio diventi parte integrante di una strategia aziendale più ampia. È evidente che oggi c'è ancora molta incertezza e probabilmente una mancanza di competenze attorno al concetto di zero trust e al suo impatto sul business. Il compito più urgente consiste nell'aiutare i leader aziendali, tra cui i CIO, a comprendere che l'obiettivo dello zero trust è quello di semplificare l'intera infrastruttura generale, eliminando l'hardware, che comporta un'intensa attività di amministrazione, e consentire alle aziende di ottenere più facilmente i risultati desiderati con i massimi livelli di sicurezza.

Esaminando le tecnologie zero trust che le aziende considerano prioritarie per gli investimenti dei prossimi dodici mesi, risulta evidente che la comprensione dei potenziali vantaggi sta migliorando, ma a un ritmo notevolmente diverso nelle varie regioni del mondo e con ampi margini di miglioramento.

PRINCIPALI TECNOLOGIE ZERO TRUST IN CUI LE ORGANIZZAZIONI STANNO INVESTENDO



PROSPETTIVA REGIONALE: LE AMERICHE

Amit Chaudhry, Senior Director, Product Marketing

Attualmente, le organizzazioni adottano il cloud, la mobilità, l'IA e le tecnologie IoT e OT per diventare più agili e competitive. Gli utenti sono distribuiti ovunque, così come i loro dati, e per una collaborazione rapida e produttiva, necessitano di un accesso diretto alle app, in qualsiasi luogo e momento.

Il ritmo esplosivo della trasformazione digitale ha fornito ai malintenzionati molteplici opportunità di sfruttare a proprio vantaggio le vecchie architetture di rete e di sicurezza.

I numeri degli attacchi sono aumentati come mai prima d'ora, in particolare per i ransomware e gli attacchi alla catena di approvvigionamento. Inoltre, man mano che le minacce diventano più sofisticate, la sicurezza basata sul perimetro, che impiega VPN e firewall, si rivela inefficace a proteggere la rete e offrire un'esperienza utente ottimale.

Per far sì che l'idea di un ambiente di lavoro flessibile e sicuro diventi la nuova realtà, le organizzazioni stanno rapidamente abbandonando i firewall e le VPN a favore dell'architettura zero trust, che è in grado di assicurare un accesso rapido e diretto alle applicazioni da qualsiasi luogo e in qualsiasi momento. Fondato sul principio dell'accesso a privilegi minimi, secondo cui la connessione viene instaurata in base all'identità e al contesto, lo zero trust è forse l'idea più semplice, ma al contempo più importante, per proteggere i dati.

È evidente che oggi c'è ancora molta incertezza e probabilmente una mancanza di competenze attorno al concetto di zero trust e al suo impatto sul business

Sezione III

Passare allo zero trust per favorire il lavoro flessibile

Un'infrastruttura a supporto del lavoro flessibile consente ai dipendenti di passare senza problemi da un ambiente di lavoro fisico a una postazione in remoto senza incorrere in limitazioni e complessità amministrative.

Quando il primo lockdown ha gettato nel caos le organizzazioni, che si affannavano per consentire ai dipendenti di lavorare da casa, non sapevamo ancora che questo "provvedimento temporaneo" avrebbe aperto la strada a un modo completamente nuovo di lavorare e che il lavoro non sarebbe mai più stato lo stesso.

La forza lavoro di oggi ha infatti a disposizione delle scelte: può lavorare da casa, dall'ufficio o da qualsiasi altro luogo, e per questo deve disporre della tecnologia necessaria per poterlo fare.

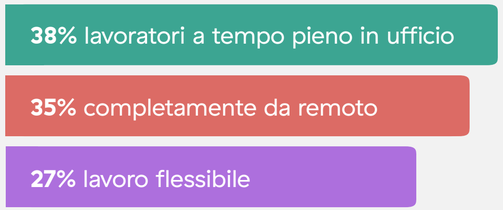
Gli intervistati hanno previsto che nei prossimi 12 mesi il personale continuerà a sfruttare appieno le diverse opzioni a disposizione, e si suddividerà tra personale in ufficio a tempo pieno (38%), completamente da remoto (35%) e flessibile (27%). Queste percentuali sono più o meno le stesse in tutto il mondo.

Se da un lato quasi due terzi (62%) dei responsabili IT affermano che il personale della propria organizzazione ha la piena flessibilità di lavorare da remoto, il fatto che più di un terzo (38%) preveda il ritorno in ufficio a tempo pieno è sorprendente e allo stesso tempo preoccupante. Sebbene possa essere comprensibile per i settori basati sulle interazioni dal vivo (come l'assistenza sanitaria e il settore alberghiero) in condizioni di mercato favorevoli, questo approccio potrebbe rendere più difficile per le aziende attrarre e trattenere nuovi professionisti, se non sono in grado di offrire l'ambiente di lavoro flessibile che i dipendenti ormai si aspettano.

19%

A livello globale, solo il 19% dei responsabili decisionali IT intervistati ha indicato che è già stata adottata un'infrastruttura zero trust per favorire il lavoro flessibile.

PERCENTUALI DELLA FORZA LAVORO A TEMPO PIENO DA REMOTO, A TEMPO PIENO IN UFFICIO O FLESSIBILE PREVISTE PER I PROSSIMI 12 MESI



Al di là dell'intenzione, la reale adeguatezza dell'infrastruttura IT e di sicurezza per gestire questa situazione in continua evoluzione è un'altra questione. A livello globale, solo il 19% dei responsabili decisionali IT intervistati ha indicato che è già stata adottata un'infrastruttura zero trust per supportare il lavoro flessibile; questo evidenzia che le organizzazioni non sono davvero pronte a gestire su larga scala questo ambiente di lavoro altamente distribuito. Accanto a coloro che hanno già aggiornato la propria infrastruttura, un ulteriore 50% ha in corso un processo di implementazione o sta pianificando di adottare una strategia basata sullo zero trust a supporto del lavoro flessibile.

Inoltre, considerando coloro che stanno implementando o pianificando l'implementazione dello zero trust per fornire un accesso remoto sicuro a fornitori, partner, collaboratori o operatori di attrezzature e stabilimenti, vale a dire chi che per sua natura lavora in un ambiente flessibile, si evince chiaramente che lo ZTNA sarà un ambito di investimento prioritario per i prossimi 12 mesi. Ci sarà quindi una forte necessità di affrontare le sfide più immediate relative al passaggio al lavoro ibrido.

Passa con il mouse sui Paesi per vedere maggiori dettagli.

L'implementazione di una strategia basata sullo zero trust per favorire il lavoro flessibile è una priorità in:

- 37% India
- 36% Singapore
- 33% Giappone
- 29% Germania
- 29% Paesi Bassi

Al contempo, i seguenti Paesi si trovano ancora prevalentemente in una fase di pianificazione:

- 34% Messico
- 27% USA
- 27% Francia
- 25% Svezia

In generale, il Regno Unito sembra essere il più riluttante ad adottare strategie zero trust a supporto del lavoro flessibile, con il 21% delle organizzazioni che afferma di non avere attualmente in programma di implementare questo tipo di infrastruttura e un ulteriore 20% che preferisce continuare a utilizzare le tradizionali tecnologie di accesso remoto.

Naturalmente, la sicurezza è una delle principali preoccupazioni per le organizzazioni sempre più flessibili.

LE PRINCIPALI PREOCCUPAZIONI LEGATE ALLA SICUREZZA DELLE ORGANIZZAZIONI CHE PASSANO AL LAVORO FLESSIBILE:

- **54%** sia i sistemi di tecnologia operativa (OT) che l'accesso a Internet
- **53%** App private on-premise o app private e carichi di lavoro sul cloud (su IaaS, PaaS)
- **32%** IoT e accesso remoto a Internet

È importante notare che questi risultati dimostrano che la sicurezza in un ambiente di lavoro flessibile non significa solamente tenere lontane le minacce, ma consiste anche nel fornire l'accesso sicuro all'infrastruttura a un ampio pool di utenti, che include dipendenti, fornitori terzi e partner commerciali.

Su questa base, nonostante la comprensibile attenzione alla sicurezza, le ragioni indicate da coloro che stanno implementando o stanno pianificando l'implementazione di un'infrastruttura zero trust iniziano anche ad alludere all'impatto più esteso per l'azienda, con implicazioni per l'esperienza e la produttività dei dipendenti.

MOTIVAZIONI PER IMPLEMENTARE O PIANIFICARE L'IMPLEMENTAZIONE DI UN'INFRASTRUTTURA ZERO TRUST PER FAVORIRE IL LAVORO FLESSIBILE

52% I dipendenti hanno esperienze di accesso diverse tra le applicazioni on-premise e le app e i dati con base cloud

46% I dipendenti subiscono un calo di produttività a causa di problemi di accesso alla rete

39% I dipendenti non sono in grado di accedere alle applicazioni e ai dati dai dispositivi personali

Passa con il mouse sui Paesi per vedere maggiori dettagli.

I paesi che segnalano maggiormente un'esperienza di accesso non uniforme sono

- 70% Giappone
- 68% India
- 64% USA
- 62% Singapore

In Europa, solo circa la metà delle organizzazioni intervistate dichiara di risentire di questa problematica, con

- 52% Svezia
- 49% Paesi Bassi
- 47% Francia
- 45% Germania

I cali della produttività dovuti ai problemi di accesso alla rete sono indicati come motivazione principale del passaggio a una nuova infrastruttura in

- 55% Messico
- 48% Spagna
- 47% Regno Unito

Gli intervistati che lavorano in aziende che si affidano ancora a infrastrutture basate su VPN per supportare il lavoro ibrido hanno riferito di essere ancora alle prese con vari problemi legati all'accesso remoto.

L'esperienza utente è fondamentale per favorire la produttività negli ambienti di lavoro flessibili: questa è la principale lezione appresa nell'ultimo anno. E i nostri risultati indicano che le regioni hanno reagito a una velocità diversa quando si è trattato di modernizzare la propria infrastruttura per risolvere gli attuali problemi dell'esperienza utente.

Per offrire un'esperienza utente ottimale negli ambienti aziendali altamente distribuiti di oggi, il traffico degli utenti deve essere indirizzato alle applicazioni sfruttando il percorso più breve possibile, per evitare latenza e congestione.

Le organizzazioni devono tenere conto della mobilità dei dipendenti flessibili di oggi, che devono essere indirizzati all'applicazione richiesta in modo dinamico e da qualsiasi luogo, con una larghezza di banda ottimizzata, che lavorino da casa, in ufficio o siano in viaggio. Oltre all'esperienza, se un dipendente non è soddisfatto delle prestazioni delle modalità di accesso alle applicazioni fondamentali per il business, potrebbe anche cercare dei modi per bypassare i controlli di sicurezza, aggravando ulteriormente l'impatto negativo potenziale.

Se facciamo un confronto, gli intervistati che lavorano in organizzazioni che cercano di supportare il lavoro flessibile con infrastrutture tradizionali basate su VPN hanno riferito di essere ancora alle prese con vari problemi legati al lavoro da remoto. Questi includono la complessità legata all'amministrazione di infrastrutture di sicurezza diverse per i dipendenti on-premise e da remoto (47%), la lentezza delle prestazioni delle applicazioni per i dipendenti (39%) e la difficoltà per l'IT di monitorare e risolvere i problemi dell'esperienza utente degli utenti in remoto (37%).

Sebbene il passaggio al lavoro flessibile sia tuttora fonte di preoccupazioni per la sicurezza, risposte come queste riflettono una sfida molto più ampia che le modalità di lavoro flessibili pongono alle organizzazioni, che include problemi di accesso, esperienza e prestazioni.

Lo zero trust, se compreso appieno, è in grado di rispondere a tutte queste esigenze, con una semplicità che consente all'IT di concentrare la propria attenzione sulle aspettative e i requisiti aziendali in continua evoluzione.

PROSPETTIVA REGIONALE: APAC

Heng Mok, CISO, Asia Pacifica e Giappone

L'Asia Pacifica (APAC) è un ottimo esempio di come una soluzione unica non sia adatta a tutti. Un melting pot di culture e stili di vita, in questa regione ogni mercato adotta un approccio diverso al lavoro. Anche prima della pandemia vi erano differenze significative: Giappone e Singapore seguivano una struttura più gerarchica, mentre Australia e India adottavano un modello di lavoro più "informale".

Dato che nella regione APAC vi sono alcune delle città che hanno subito più lockdown a livello globale, queste sfumature sono ancora più accentuate ora che stiamo uscendo da questa fase. Tra gli intervistati, la maggior parte dei responsabili decisionali IT provenienti dal Giappone e da Singapore si aspettava un rientro a tempo pieno in ufficio, in netto contrasto con gli intervistati di Australia e India, che prevedevano di adottare un modello completamente in remoto.

Tuttavia, nel lungo periodo, riteniamo che sempre più organizzazioni intensificheranno il supporto di modelli di lavoro flessibili. Molte delle aziende con cui ho avuto modo di confrontarmi stanno optando per approcci di lavoro flessibili, in modo da sfruttare i vantaggi derivanti dalla capacità di attrarre e trattenere professionisti qualificati. Con l'aumento della concorrenza da un lato e il ristretto numero di talenti dall'altro, non sorprende che molti stiano adottando politiche analoghe e cercando di adattare gli stack tecnologici a questa transizione.

L'esperienza utente è fondamentale per favorire la produttività negli ambienti di lavoro flessibili: questa è la principale lezione appresa nell'ultimo anno.

Sezione IV

Adottare un approccio zero trust per integrare le tecnologie emergenti

Le tecnologie emergenti sono le tecnologie nuove o in rapido sviluppo, le cui applicazioni pratiche sono ancora in gran parte non concretizzate, ma che si prevede avranno un impatto significativo sulle aziende e determineranno un vantaggio competitivo.

Naturalmente, le soluzioni digitali a supporto del lavoro a distanza non sono le uniche tecnologie verso cui le organizzazioni stanno volgendo il loro interesse. Nell'era digitale di oggi, la tecnologia operativa svolge un ruolo sempre più determinante. Questo segmento del modello di business di un'organizzazione, che storicamente faceva prevalentemente affidamento su sistemi e processi legacy, vedrà un cambiamento radicale grazie all'adozione di nuove tecnologie emergenti, che consentiranno di semplificare e automatizzare ulteriormente i processi aziendali.

Ma le organizzazioni devono guardare ancora più lontano e prendere in considerazione anche gli altri progressi tecnologici in arrivo per far sì che le proprie decisioni infrastrutturali siano ancora più lungimiranti. I responsabili decisionali IT devono considerare le varie direzioni in cui l'azienda può andare, tenendo conto delle varie innovazioni e mantenere una mentalità aperta per comprendere il modo in cui le tecnologie emergenti potranno supportare il business in modo efficace. Lo zero trust può essere l'anello mancante e aiutare le aziende a ottenere gli strumenti necessari per prepararsi sin da subito alle tecnologie future.

In linea con le motivazioni alla base della migrazione al cloud e della trasformazione digitale in generale, i nostri dati hanno rivelato che l'attenzione verso l'ottenimento di risultati strategici più ampi sembra mancare nella pianificazione dei progetti legati alle tecnologie emergenti delle organizzazioni.

Alla domanda su quale sia l'aspetto più impegnativo nell'implementazione di progetti legati alle tecnologie emergenti, il 30% indica una sicurezza adeguata, seguita dai requisiti di budget per far progredire la digitalizzazione (23%). Tuttavia, solo il 19% cita come sfida la dipendenza dalle decisioni strategiche di business.

L'ASPETTO PIÙ DIFFICILE DELL'IMPLEMENTAZIONE DI PROGETTI LEGATI ALLE TECNOLOGIE EMERGENTI PER REGIONE

Passa con il mouse sui Paesi per vedere maggiori dettagli.

Le preoccupazioni per la sicurezza rappresentano la sfida principale nei seguenti paesi

- 54% Brasile
- 41% Giappone
- 37% India
- 37% Italia
- 35% Spagna
- 31% USA

I seguenti Paesi stanno invece lottando prevalentemente con i requisiti di budget:

- 27% Singapore
- 27% Francia
- 23% Regno Unito

La mancanza di lungimiranza sembra essere il principale ostacolo che si frappone tra le organizzazioni e le tecnologie emergenti.

- 24% Paesi Bassi

L'unico paese in cui la maggior parte delle aziende ha indicato la dipendenza dalle decisioni strategiche di business come l'ostacolo più grande

- 28% Svezia

Anche se le preoccupazioni sul budget sono prevedibili, è interessante notare l'attenzione rivolta alla protezione della rete e il mancato interesse verso l'allineamento strategico con il business. Le organizzazioni si concentrano sulla sicurezza senza comprendere appieno i vantaggi aziendali derivanti della sicurezza stessa, a riprova del fatto che lo zero trust non viene ancora concepito come fattore abilitante per il business.

Nella pianificazione dei casi d'uso delle tecnologie emergenti, come la realtà aumentata, il gemello digitale e le costruzioni virtuali, un'ulteriore preoccupazione è quella relativa all'accesso a bassa latenza e ad alte prestazioni alle applicazioni. Questo vale soprattutto per le Americhe, dove l'interesse per le tecnologie emergenti nei prossimi tre anni sarà particolarmente elevato.

RILEVANZA DELL'ACCESSO A BASSA LATENZA E AD ALTE PRESTAZIONI ALLE APPLICAZIONI NEI PROSSIMI TRE ANNI

PRINCIPALI TECNOLOGIE PRIORITARIE ENTRO IL 2025	GLOBALE	EUROPA	AMERICA	APAC
Accesso con base cloud ai sistemi di tecnologia operativa e controllo industriale	34%	29%	40%	38%
Implementazione della tecnologia 5G per una migliore connettività	32%	29%	39%	32%
Riduzione dell'impronta di carbonio dell'azienda	29%	28%	28%	30%
Implementazione di progetti di intelligenza artificiale/ machine learning	27%	22%	39%	28%

Passa con il mouse sui Paesi per vedere maggiori dettagli.

Organizzazioni che puntano sull'accesso cloud a OT e controllo industriale:

- 46% Messico
- 45% India
- 44% Singapore
- 36% Australia
- 33% Francia

Organizzazioni che danno la priorità all'implementazione delle tecnologie 5G:

- 47% Brasile
- 45% India
- 41% Italia
- 36% Spagna
- 28% Regno Unito

Organizzazioni che indicano la riduzione dell'impronta di carbonio come priorità principale:

- 41% Italia
- 28% Germania
- 32% Svezia

Solo le organizzazioni dei Paesi Bassi considerano più importante l'espansione dell'edge computing (29%), mentre gli Stati Uniti si stanno concentrando molto sull'implementazione di progetti basati su IA e ML (43%).

Possiamo già iniziare a immaginare come queste tecnologie emergenti prioritarie potrebbero portare le aziende a ottenere risultati in più aree. Tuttavia, i nostri dati evidenziano ancora la mancanza di una visione più lungimirante all'interno delle organizzazioni. All'interno delle aziende, è necessario un allineamento molto più consapevole riguardo ai vantaggi competitivi che si possono ottenere grazie alle tecnologie emergenti e al loro impiego strategico, che ovviamente tenga anche in considerazione il modo in cui proteggere questi nuovi strumenti.

PROSPETTIVA REGIONALE: EMEA

Nathan Howe, VP of Emerging Technology

Le organizzazioni europee sono meno propense a fare il primo passo per l'adozione di tecnologie nuove o emergenti. Anche se l'Europa è stata la culla della rivoluzione industriale con le invenzioni meccaniche, questa regione è stata superata ormai da molto tempo per quanto riguarda l'adozione di tecnologie digitali. L'area dell'Asia Pacifica e del Giappone è diventata il centro principale per la realizzazione di chip, mentre la Silicon Valley riunisce le conoscenze di persone provenienti da tutto il mondo che lavorano per sviluppare tecnologie trasformative.

Non sorprende quindi che l'Asia abbia già riconosciuto la potenza del 5G per andare oltre il wireless e passare a un nuovo livello di connettività come base per la digitalizzazione. Mentre le Americhe si trovano in una posizione intermedia, l'Europa è ancora incerta su come passare al 5G nelle proprie attività di digitalizzazione. Tuttavia, l'Europa è pronta a crescere drasticamente nell'ambito del cloud digitale e delle tecnologie emergenti, dato che le tendenze geopolitiche attuali, come la carenza di chip e i problemi della catena di approvvigionamento, stanno spingendo i vari paesi a creare centri di eccellenza interni alla regione.

Sezione V

La strada per realizzare il pieno potenziale dello zero trust

In base a questi risultati, in che modo le organizzazioni dovrebbero affrontare i loro percorsi verso lo zero trust?

Le annose problematiche delle architetture di rete e sicurezza legacy richiedono di rivoluzionare le modalità attraverso cui viene concessa la connettività nel mondo moderno. È proprio qui che va sfruttata l'architettura zero trust, che non considera nessun utente e nessuna applicazione automaticamente attendibili. Lo zero trust si basa sul principio dell'accesso a privilegi minimi, che garantisce che l'attendibilità venga concessa solo dopo aver verificato l'identità e il contesto e dopo aver applicato i controlli delle policy.

Questo approccio tratta tutte le comunicazioni di rete come ostili, e le comunicazioni tra utenti e carichi di lavoro o tra carichi di lavoro vengono bloccate fino a quando non vengono convalidate da policy basate sull'identità. In questo modo, si evitano gli accessi inopportuni e il movimento laterale. Questa convalida si applica a qualsiasi ambiente di rete, e la posizione sulla rete di un'entità non rappresenta più un fattore rilevante; di conseguenza, si elimina la dipendenza da una segmentazione rigida della rete.

Lo zero trust è nato come un modo nuovo di proteggere le reti e in seguito si è esteso oltre le reti on-premise, seppur rimanendo ancora concentrato prevalentemente sulla protezione del traffico delle applicazioni private. Per troppo tempo il traffico è stato valutato in base al suo rapporto con la rete, ma la rete andrebbe eliminata dalla considerazione. Oggi, le organizzazioni devono essere consapevoli del pieno potenziale dello zero trust, per proteggere le applicazioni SaaS, il traffico da e verso i cloud pubblici e persino gli utenti che accedono alla rete Internet pubblica. Le fonti di questo traffico possono essere sia i carichi di lavoro che gli utenti. L'accesso può essere reso indipendente dal mezzo di trasporto, e il traffico può passare attraverso qualsiasi router e attraverso qualsiasi rete, cablata o wireless, 4G o 5G e future estensioni.

È ormai giunto il momento di applicare i principi dello zero trust a tutto il traffico, indipendentemente dall'origine e dalla destinazione. È ora di smettere di pensare quale entità si sta connettendo a quale rete, e utilizzare invece lo zero trust per connettere tutte le entità in modo diretto, utilizzando le policy aziendali. Nell'epoca del cloud, Internet è la nuova rete aziendale, e tutto il traffico rappresenta un potenziale bersaglio.

Quali sono i passi che le organizzazioni possono iniziare a compiere oggi stesso per assicurarsi di diventare aziende sicure, agili, flessibili ed efficienti ed essere in linea non solo con gli ambienti macroeconomici di oggi, ma anche con i requisiti delle tecnologie emergenti?

Ci sono tre raccomandazioni principali:

1

Le organizzazioni devono riconsiderare la loro idea di zero trust e vederlo come un fattore trainante per ottenere una trasformazione digitale sicura e supportare i risultati aziendali

Grazie ai livelli di visibilità e controllo più elevati che offre, un'architettura basata sullo zero trust elimina la complessità dell'IT moderno e consente alle organizzazioni di concentrarsi sull'ottenimento dei risultati attesi dalla loro tecnologia, con prestazioni elevate, un'esperienza utente ottimale e la riduzione dei costi.

2

È necessaria una formazione più avanzata, per dissipare paure, incertezze e dubbi attorno al concetto di zero trust e al suo reale impatto sul business

I CIO e i CISO hanno il ruolo fondamentale di comunicare in modo più completo i vantaggi dello zero trust ai consigli di amministrazione concentrandosi sul modo in cui questo approccio si allinea alla strategia aziendale.

3

Le tecnologie emergenti devono essere considerate un vantaggio competitivo per il business, e le infrastrutture zero trust devono gettare oggi le basi per il futuro

La decisione su quali tecnologie emergenti adottare deve essere guidata dalla visione aziendale complessiva e dalle esigenze attuali e future dell'organizzazione, non dalle tendenze o da ciò che va più di moda in un particolare momento. Lo zero trust supporta i requisiti di connettività sicura e performante delle tendenze emergenti.

Quindi, quando la mentalità sarà cambiata e il potenziale dello zero trust riconosciuto, come dovranno procedere le organizzazioni all'implementazione di un'architettura zero trust che consenta di conseguire questi obiettivi aziendali?

Zscaler ha implementato lo zero trust come componente architetturale fondante della piattaforma Zero Trust Exchange, ed è alla base di ogni elemento del framework SSE. Questo significa che applica lo zero trust agli utenti che accedono a qualsiasi applicazione (interna o esterna), alla connettività IoT/OT e ai carichi di lavoro che accedono alle risorse in un ambiente multicloud o sulla rete Internet stessa. I principi dello zero trust consentono alle aziende di offrire la possibilità a dipendenti, partner commerciali e clienti di lavorare in modo flessibile, sicuro e produttivo da qualsiasi luogo, un requisito fondamentale per la continuità aziendale, l'acquisizione di professionisti in remoto e la sempre maggiore popolarità degli ambienti di lavoro ibridi.

Zscaler Zero Trust Exchange è un servizio nativo del cloud che fornisce a dipendenti, partner e clienti un accesso rapido, diretto e sicuro alle applicazioni esterne e interne, indipendentemente dalla posizione, dal dispositivo o dalla rete.

Inoltre, integra i sette elementi essenziali dell'architettura zero trust, che sono raggruppati nelle seguenti tre categorie:

Verifica

L'architettura zero trust prima di tutto interrompe la connessione e stabilisce:

1. Chi si sta connettendo?
2. Qual è il contesto dell'accesso?
3. Qual è la destinazione della connessione?

Controllo

L'architettura zero trust procede quindi a:

4. Valutare il rischio
5. Prevenire le compromissioni
6. Prevenire la perdita di dati

Applicazione

Infine, prima di stabilire la connessione, l'architettura zero trust:

7. Applica le policy

Questi elementi consentono alle organizzazioni cloud-first di gettare le basi per accelerare la trasformazione digitale e diventare aziende pronte ad affrontare il futuro.

Informazioni su Zscaler e Zscaler Zero Trust Exchange

Con la piattaforma zero trust più ampia, facile da usare e avanzata, Zscaler è universalmente riconosciuta come leader del settore.

La piattaforma nativa del cloud Zscaler Zero Trust Exchange può supportare il tuo percorso verso lo zero trust. A differenza dei prodotti di rete e di sicurezza legacy, Zero Trust Exchange è una piattaforma cloud creata ad hoc, dove la sicurezza inizia con l'interruzione di tutte le connessioni e consente un'ispezione approfondita dei contenuti e la verifica dei diritti di accesso in base all'identità e al contesto.

La soluzione Zero Trust Exchange viene eseguita in 150 data center in tutto il mondo, per garantire che il servizio sia vicino agli utenti e affianchi i provider cloud e le applicazioni a cui accedono, come Microsoft 365 e AWS. Garantisce inoltre il percorso più breve tra gli utenti e le rispettive destinazioni, offrendo una sicurezza completa e un'esperienza utente ottimale.

Puoi scoprire di più sulla nostra piattaforma facile da usare qui.

Zero Trust Exchange opera attraverso 150 data center in tutto il mondo

Metodologia

ATOMIK Research ha intervistato 1908 responsabili decisionali di livello senior (CIO/CISO/CDO/responsabili dell'architettura di rete) nell'area EMEA (Regno Unito, Germania, Francia, Paesi Bassi, Svezia, Italia, Spagna), Americhe (USA*, Messico, Brasile) e APAC (Giappone, India, Australia, Singapore). La ricerca è stata condotta tra il 31 maggio e il 28 giugno del 2022. Il campione comprende per il 43% organizzazioni con un numero di dipendenti fino a 4999, per il 32% organizzazioni con un numero di dipendenti da 5000 a 9999, e per il 25% organizzazioni con 10.000 o più dipendenti.