ivanti

Cybersecurity
INSIDERS

Report 2021
sui progressi Zero Trust

ivanti.com

Panoramica

L'adozione da parte delle aziende del modello di sicurezza zero trust sta guadagnando slancio: la maggior parte delle aziende prevede infatti di implementare funzionalità zero trust per mitigare il crescente rischio informatico, soprattutto a seguito del passaggio al lavoro da remoto. Con il suo principio di verifica dell'utente e del dispositivo prima di concedere l'accesso condizionale in base al livello minimo di autorizzazioni, zero trust mantiene la promessa di usabilità, protezione dei dati e governance notevolmente migliorate.

Il report 2021 sull'approccio zero trust rivela come le aziende stiano implementando sistemi di sicurezza zero trust e presenta fattori chiave, tendenze di adozione, tecnologie, investimenti e vantaggi.

Per raccogliere queste informazioni, abbiamo intervistato professionisti della sicurezza informatica, dai dirigenti tecnici ai professionisti IT, rappresentativi di una sezione trasversale equilibrata di aziende di varie dimensioni in più settori.

I risultati chiave includono:

- La fiducia guadagnata attraverso la verifica delle entità (come utenti, dispositivi e componenti d'infrastruttura) (64%) rappresenta l'aspetto principale di un approccio zero trust, seguita da protezione dei dati (63%) e autenticazione/autorizzazione continua (61%);
- Determinare le autorizzazioni di accesso attuali per tutti gli utenti può essere un compito arduo, per assicurarsi chea gli utenti vengano assegnati i livelli di accesso appropriati. Più di 3/4 delle aziende (88%) riconoscono che è probabile che gli utenti dispongano di autorizzazioni di accesso superiori alle loro effettive esigenze;
- Alla domanda sulle loro attuali priorità in termini di sicurezza, i professionisti della sicurezza informatica hanno indicato il miglioramento della gestione di identità e accessi (68%), seguito dalla prevenzione della perdita di dati (56%) e dall'accesso sicuro alle applicazioni (46%).

Un grazie particolare a Ivanti per aver sostenuto questo importante progetto di ricerca.

Ci auguriamo che le informazioni contenute in questo report ti siano utili nel tuo impegno continuo volto a proteggere i tuoi ambienti IT.

Grazie,

Holger Schulze
AD e fondatore
Cybersecurity Insiders

Cybersecurity
INSIDERS

Holger Schulze

Principi Zero Trust

Abbiamo chiesto alle aziende quali aspetti dell'approccio zero trust trovano più convincenti. La fiducia guadagnata attraverso la verifica delle entità (come utenti, dispositivi e componenti dell'infrastruttura) (64%) è al primo posto tra gli aspetti principali di una strategia zero trust. Seguono la protezione dei dati (63%) e l'autenticazione/autorizzazione continua (61%).

Quali principi zero trust sono più convincenti per te e la tua azienda?[1]

64%

Fiducia ottenuta attraverso la verifica delle entità (ad es. utente, dispositivo, infrastruttura)

63%

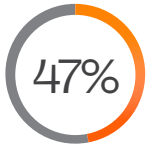
Protezione dei dati (ad es. connessione sicura)

61%

Autenticazione/ autorizzazione continua

Visibilità e verifica degli accessi end-to-end

Semplificazione dell'accesso con autorizzazioni minime



Criterio di accesso centralizzato e granulare

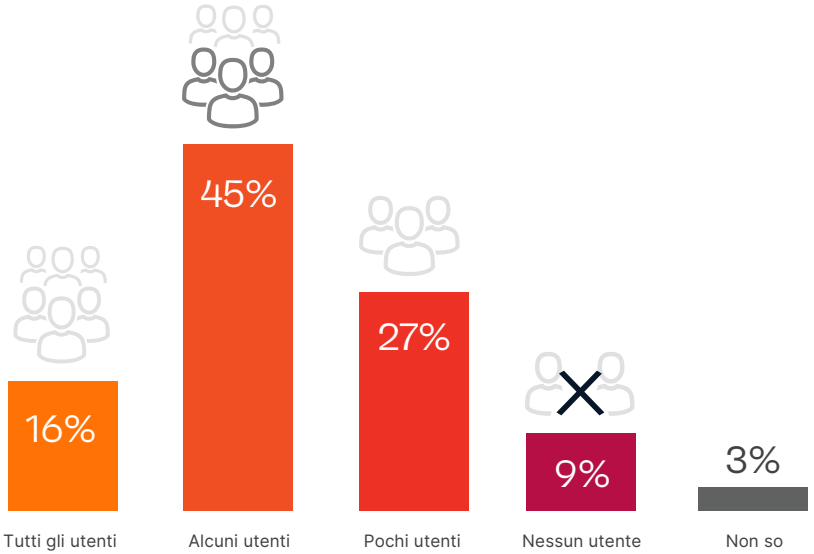
Nessuna distinzione di fiducia tra rete interna o esterna

Autorizzazioni di accesso eccessive

Determinare le autorizzazioni di accesso attuali per tutti gli utenti può essere un compito arduo, per assicurarsi che vengano assegnati loro i livelli di accesso appropriati. Più di 3/4 delle aziende (88%) riconoscono che è probabile che gli utenti dispongano di autorizzazioni di accesso superiori alle loro effettive esigenze.

Fino a che punto ritieni che gli utenti della tua azienda dispongano di autorizzazioni di accesso superiori alle loro effettive esigenze?

88% ha riconosciuto che probabilmente gli utenti dispongono di autorizzazioni di accesso superiori alle loro effettive esigenze.



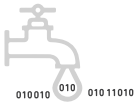
Priorità di sicurezza

Alla domanda sulle loro attuali priorità in termini di sicurezza, i professionisti della sicurezza informatica indicano il miglioramento della gestione di identità e accessi (68%), seguito dalla prevenzione della perdita di dati (56%) e dall'accesso sicuro alle applicazioni (46%).

Quali sono, per la tua azienda, le attuali priorità in termini di sicurezza?[2]

68%

Migliorare la gestione delle identità e degli accessi (IAM)

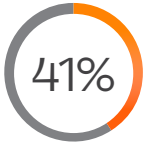


56%

Prevenzione della perdita di dati (DLP)

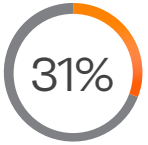
46%

Garantire l'accesso sicuro alle applicazioni ospitate su servizi cloud di altri fornitori
(ad es. Microsoft, Amazon, Google)



Abilitare Endpoint Mobile Management (EMM)/BYOD
(ad es. utenti, dispositivi)

Condurre un'ispezione SSL approfondita
(ad es. decrittografia sicura della sessione per la scansione di malware e filtraggio web/e-mail)



Semplificare la fornitura di accessi sicuri
(ad es. esperienza utente, amministrazione)

Aumentare o sostituire gli strumenti di accesso remoto esistenti
(ad es. VDI, VPN, RDP)

Priorità per accesso basato su identità e Zero Trust

Abbiamo chiesto alle aziende in quali controlli di sicurezza per accesso basato sull'identità e zero trust stanno investendo. Al primo posto, dal punto di vista degli investimenti, è l'autenticazione a più fattori (58%), seguita dalla gestione e governance delle identità (48%) e dal single-sign-on (45%).

Quale dei seguenti controlli per accesso basato su identità/zero trust è considerato prioritario, in termini di investimenti, nella tua azienda nei prossimi 12 mesi?[3]

58%

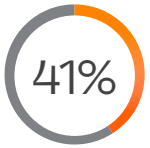
Autenticazione a più fattori (MFA)

48%

Gestione e governance delle identità

45%

Single Sign-On (SSO)



Gestione degli accessi privilegiati (PAM), microsegmentazione

Reti private virtuali (VPN)

Microsegmentazione

Controllo dell'accesso alla rete (NAC), Web Application Firewall (WAF)

Priorità per accesso sicuro

Analizzando nel dettaglio le specifiche priorità per quanto riguarda l'accesso sicuro, le aziende danno nuovamente precedenza all'autenticazione a più fattori/gestione degli account privilegiati (69%). Seguono il rilevamento e la risposta ad attività anomale (58%) e la protezione dell'accesso da dispositivi personali non gestiti (55%).

Quali sono le priorità per l'accesso sicuro della tua azienda per i prossimi 12-24 mesi?

69%

Autenticazione a più fattori/Gestione account privilegiati

58%

Rilevamento e risposta ad attività anomale

55%

Protezione dell'accesso da dispositivi personali non gestiti

Rivalutare l'infrastruttura di sicurezza legacy e prendere in considerazione l'accesso

Maggiori visibilità e metriche di sicurezza per i dirigenti

Microsegmentazione

Sfide relative all'accesso sicuro

Nella protezione dell'accesso ad app e risorse, viene data particolare attenzione all'accesso con privilegi eccessivi (60%), seguito dalla fornitura di un accesso sicuro ai partner (50%): entrambe queste sfide sono affrontate direttamente da una strategia zero trust.

Quali sono le principali sfide che la tua azienda deve affrontare per garantire l'accesso ad applicazioni e risorse?

60%

Accesso dei dipendenti con privilegi eccessivi

50%

Partner che accedono in modo non sicuro ad app e risorse

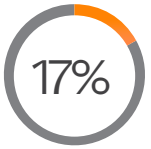
47%

Attacchi informatici
(ad es. denial of service, scripting tra siti, man-in-the-middle, phishing)

Shadow IT

I processi manuali sono complessi e rallentano la capacità di reagire rapidamente

Accesso alle risorse da parte di dispositivi mobili vulnerabili, sottoposti a jailbreak o smarriti

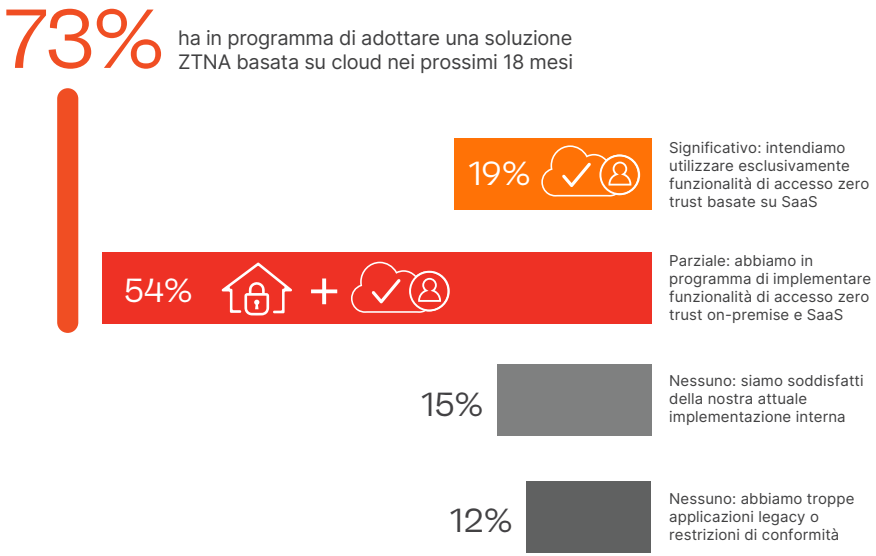


ccesso alle risorse di rete da parte di dispositivi a rischio
(endpoint sconosciuti, non autorizzati, non conformi)

Zero Trust SaaS

La sicurezza si sta spostando sul cloud e le soluzioni ZTNA non fanno eccezione. Quasi tre quarti degli intervistati pianificano di adottare una soluzione ZTNA basata su cloud nei prossimi 18 mesi.

Nei prossimi 18 mesi, fino a che punto tu e la tua azienda prevedete di adottare funzionalità di accesso Zero Trust in modalità SaaS?



Accesso alle app private

Abbiamo chiesto alle aziende quali sono le sfide più grandi per quanto riguarda la protezione delle app private. Per più della metà degli intervistati, l'accesso sicuro alle applicazioni distribuite in ambienti cloud pubblici rappresenta attualmente la problematica maggiore (54%).

Per quanto riguarda la protezione dell'accesso alle app private, ordina gli aspetti seguenti partendo da quello che rappresenta attualmente la problematica maggiore.

54% Accesso alle app nel cloud pubblico

29% Accesso alle app nel mio data center

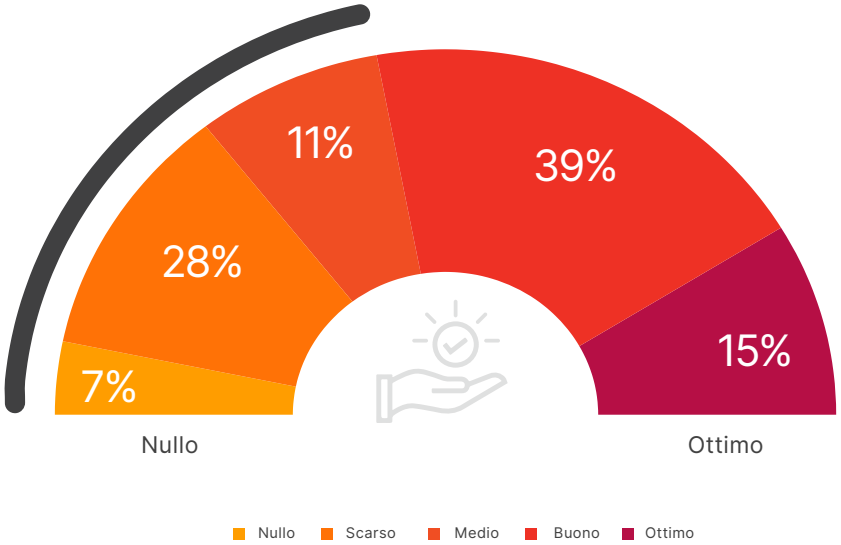
17% Accesso alle app nella mia sede

Fiducia nelle proprie capacità Zero Trust

Alla domanda sul livello di fiducia nelle proprie capacità di applicare una strategia zero trust, quasi la metà dei team di sicurezza IT aziendale ammette di non ritenere di essere in grado (46%).

Qual è il tuo livello di fiducia nelle tue capacità di applicare un modello/principi completamente zero trust nella tua architettura di accesso sicuro?

46% dei team di sicurezza IT aziendale non ha fiducia nella propria capacità di applicare una strategia zero trust



Accesso alle app negli ambienti cloud pubblici

Le tradizionali soluzioni di accesso remoto non soddisfano i requisiti degli ambienti cloud dinamici e distribuiti di oggi. Alla domanda sugli scenari che i professionisti della sicurezza informatica incontrano quando forniscono un accesso sicuro, la soluzione più citata è “l’hairpinning” degli utenti remoti e mobili attraverso i data center per accedere agli ambienti cloud pubblici per le app (47%). Un allarmante 37% deve esporre pubblicamente le app cloud per consentire agl utenti remoti e mobili di utilizzarle, introducendo così un rischio significativo.

Quale dei seguenti scenari hai riscontrato nel fornire accesso sicuro alle app su cloud pubblico per utenti remoti o mobili?

47%

Sono costretto a effettuare "l'hairpinning" degli utenti remoti attraverso i miei data center per accedere alle app nel cloud pubblico

37%

Devo esporre pubblicamente le mie app private nel cloud pubblico per fornire l'accesso

35%

Non riesco a distribuire il mio dispositivo VPN remoto preferito in ambienti cloud pubblici

Fattori a favore di una strategia Zero Trust

Cosa spinge le aziende ad avviare o realizzare una strategia zero trust? Al primo posto, la sicurezza dei dati con l'82%, seguita dalla prevenzione delle violazioni (68%) e dalla riduzione delle minacce agli endpoint (53%).

Quali sono per la tua azienda i fattori chiave per avviare o potenziare una strategia di accesso basato sull'identità/zero trust?[4]

82%

Sicurezza/protezione dei dati

68%

Prevenzione delle violazioni

53%

Ridurre le minacce alla sicurezza degli endpoint e dell'IoT

Ridurre le minacce interne

Conformità normativa/di settore (ad es. HIPAA, GDRP, PCI DSS)

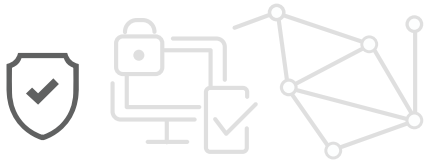
Risoluzione dei problemi di sicurezza dell'IT ibrido

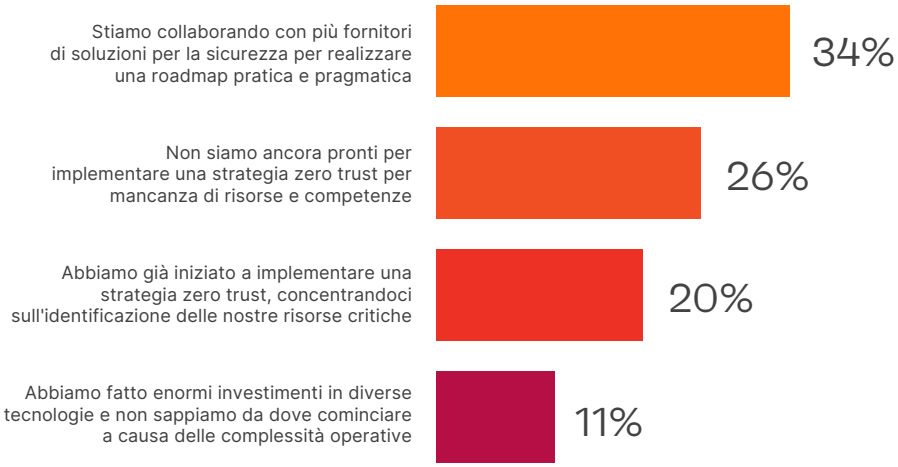
Efficienza operativa

Implementazione Zero Trust

Le soluzioni zero trust stanno rapidamente guadagnando slancio e le aziende seguono strade diverse nell'implementazione della tecnologia. L'approccio più comune adottato dalle aziende è quello di collaborare con più fornitori di soluzioni per la sicurezza, per realizzare una roadmap di implementazione pratica e pragmatica (34%). Tuttavia, la mancanza di risorse e competenze (26%) rimane un ostacolo significativo.

Se l'implementazione di una strategia zero trust è un processo graduale, come pensi d'implementarla nel tuo ambiente esteso?[5]

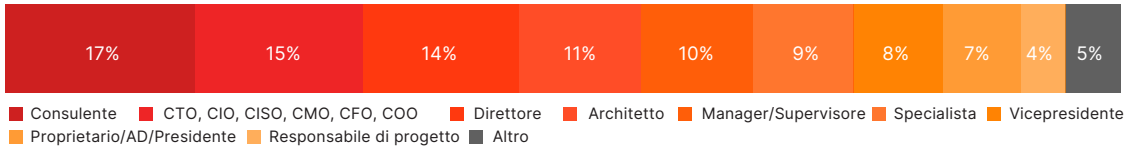




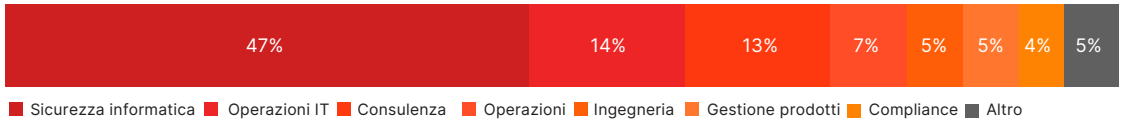
Methodology and Demographics

Questo report si basa sui risultati di un sondaggio online completo, condotto nel luglio del 2021, a cui hanno partecipato 443 professionisti IT e di sicurezza informatica negli Stati Uniti, volto a identificare le ultime tendenze, sfide, lacune e preferenze di soluzioni nell'adozione da parte delle aziendale di soluzioni relative alla sicurezza zero trust. Le persone persone intervistate vanno da dirigenti tecnici a professionisti della sicurezza IT, e rappresentano una sezione trasversale equilibrata di aziende di varie dimensioni in più settori.

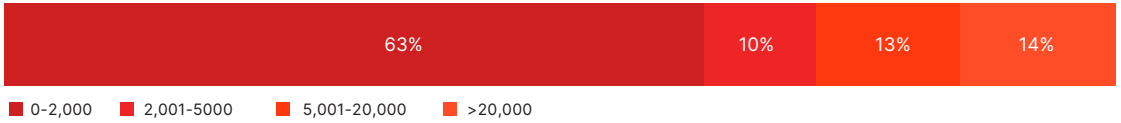
Profilo professionale



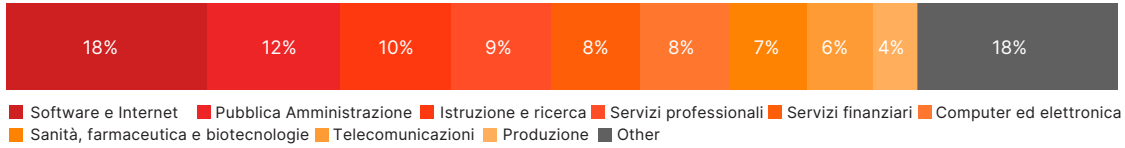
Reparto



Dimensioni azienda



Settore



ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

Ivanti rende possibile l'Everywhere Workplace. Con l'Everywhere Workplace, i dipendenti utilizzano una miriade di dispositivi per accedere ad applicazioni e dati IT su varie reti per rimanere produttivi da qualsiasi luogo essi lavorino.

La piattaforma di automazione Ivanti Neurons raccoglie le soluzioni di gestione unificata degli endpoint, sicurezza Zero Trust e gestione dei servizi aziendali migliori del settore, per offrire un'unica piattaforma IT con funzioni di riparazione e protezione automatica dei dispositivi, e assistenza self-service per gli utenti finali.

Oltre 40.000 clienti, fra i quali 78 delle aziende Fortune 100, hanno scelto Ivanti per individuare, gestire, mettere in sicurezza ed erogare serivizi alle loro risorse IT dal cloud all'edge, e offrire al contempo esperienze ottimali ai loro dipendenti, indipendentemente da dove e come lavorono.

Per maggiori informazioni,
visita ivanti.com e segui @GoIvanti.

1 Segregazione delle risorse 40% | Altro 2%
2 Migliorare rilevamento e risposta degli endpoint (EDR) 28% | Migliorare le funzioni di sicurezza SD-WAN 27% | Migliorare la correzione delle vulnerabilità (ad es. gestione delle vulnerabilità, gestione delle patch) 5% | Fornire una migliore protezione dalle minacce mobili (difesa dalle minacce mobili/anti-phishing) 2% | Nessuno 2% | Altro 4%
3 Web Application Firewall (WAF) 35% | Gestione mobile aziendale (MDM) 31% | Cloud Access Security Broker (CASB) 30% | Analisi dell'identità 27% | Software Defined Perimeter (SDP) 26% | Servizi di directory aziendali 17% | Controllo completo sull'accesso alla rete Zero Trust 12% | Gestione vulnerabilità/ gestione patch 9% | Invisibilità dei dispositivi di rete alle minacce 7% | Anti-phishing 7% | Difesa dalle minacce mobili 5% | Altro 2%
4 Conformità interna 28% | Risposta a audit o a incidente di sicurezza 28% | Altro 5%
5 Altro 9%