Akamai

WHITE PAPER

Un piano per Zero Trust Network Access

A chi è destinata questa guida?

Architetti di rete, tecnici della sicurezza, CTO, CISO e altri responsabili IT e decisionali potranno trarre vantaggio dalla lettura di questa guida.

Questa guida fornisce ai responsabili di definizione dell'ambito, configurazione, distribuzione, implementazione e gestione di un progetto Zero Trust Network Access (ZTNA) un'analisi completa dei potenziali vantaggi e delle differenze tra i vari sistemi. La guida include informazioni su:

- Limitazioni e problemi di sicurezza negli approcci tradizionali all'accesso alle applicazioni e motivi per cui è richiesta la soluzione ZTNA
- I componenti della soluzione ZTNA e il suo funzionamento
- Come Akamai Enterprise Application Access e Akamai MFA possono fornire la soluzione ZTNA in modo rapido e semplice

Con i cambiamenti del mondo aziendale e l'aumento delle minacce informatiche, le imprese stanno adottando un nuovo approccio alle loro difese informatiche. Molte aziende hanno compreso che la tradizionale architettura di rete, basata su una posizione centralizzata in cui tutti gli utenti possono accedere alle applicazioni, le rende vulnerabili. Questo approccio alla sicurezza, riferito a un modello che vedeva l'organizzazione come un castello da difendere attraverso la costruzione di mura e fossati per proteggere il perimetro aziendale supponendo che tutti al suo interno fossero al sicuro, espone le aziende al rischio di subire attacchi informatici nell'odierno scenario delle connessioni mobili e del cloud. Al contrario, le aziende lungimiranti stanno adottando il concetto di un'architettura Zero Trust per proteggere le loro risorse più importanti. Un principio fondamentale in ogni progetto Zero Trust è rappresentato dalla protezione della rete. In questo white paper, viene descritta l'inadeguatezza dei tradizionali approcci alla sicurezza della rete hub e spoke e si spiega come il passaggio alla soluzione ZTNA consenta di difendere meglio le risorse di importanza critica, fungendo da cardine verso l'adozione di un'architettura Zero Trust completa.

Il ritmo dei cambiamenti aziendali non è mai stato così veloce

Il modo con cui le aziende ricorrono alla tecnologia e la usano cambia in continuazione e con una rapidità eccezionale. L'evoluzione del computing ha favorito una rapida transizione da uno scenario in cui le applicazioni aziendali erano ospitate nei data center on-premise all'utilizzo di più cloud pubblici, di cloud privati o di un approccio ibrido (on-premise e cloud pubblici/privati).

L'evoluzione del modello aziendale ha anche favorito una maggiore collaborazione tra le entità coinvolte e la necessità di offrire a partner e fornitori l'accesso alle applicazioni e alle risorse desiderate.

Infine, man mano che le aziende continuano ad adottare il lavoro remoto o ibrido, gli utenti si trovano sempre più ad accedere alle applicazioni e alle risorse aziendali ovunque, su dispositivi gestiti o meno.

Con questi cambiamenti, gli approcci tradizionali alla gestione dell'accesso alle applicazioni non sono più sufficienti, pertanto le aziende devono ora ricorrere a nuove soluzioni, che offrano un accesso sicuro indipendentemente dalle posizioni in cui sono ospitate le applicazioni o in cui si trovano gli utenti.

Accesso alle applicazioni di tipo tradizionale

Per oltre 20 anni, le aziende si sono affidate ai firewall per costruire un solido perimetro di sicurezza, considerando attendibili gli utenti che si trovavano al suo interno. Questo approccio considera le reti come castelli circondati da fossati: mura spesse e cancelli ben protetti formano il perimetro che protegge il castello (o, in tal caso, la rete), a cui possono accedere solo gli utenti con le giuste credenziali. Una volta all'interno, gli utenti possono quindi accedere a specifiche applicazioni in base alla loro identità, che viene fornita tramite soluzioni IdP (Identity Provider) come Microsoft Active Directory.

Tuttavia, con le reti flat, gli utenti possono ottenere l'accesso IP a tutta la rete e, di conseguenza, individuare altri server e altre applicazioni. Ad esempio, con una soluzione IdP configurata correttamente, un utente che trova il server su cui viene ospitata l'applicazione per le buste paga e accede all'applicazione, viene respinto.

Per risolvere il problema del movimento laterale privo di restrizioni, le applicazioni hanno avviato la partizione delle applicazioni in segmenti separati dietro a un firewall tramite le VLAN (Virtual Local Access Network) e hanno applicato le ormai arcaiche regole basate sugli intervalli IP per utenti singoli o gruppi. Questo processo è precario e decisamente soggetto ad errori. Consideriamo il caso in cui qualcuno sta effettuando la manutenzione dei computer e li sta spostando in un nuovo rack oppure deve spostare nuovamente i loro IP su un nuovo intervallo. All'improvviso, tutti gli utenti si ritrovano bloccati e le telefonate di assistenza arrivano a raffica. Oppure, consideriamo l'esempio in cui l'architettura di un'applicazione cambia durante un aggiornamento del software e gli utenti vengono reindirizzati su un altro computer come parte del workflow, ma quel computer è inaccessibile per determinati utenti o gruppi perché le regole del firewall non sono state aggiornate.

Questa architettura è estremamente complessa e richiede un livello molto elevato di comunicazione tra proprietari delle applicazioni, amministratori di rete e gruppi di sicurezza durante le modifiche per assicurare che non si verifichino problemi di downtime.

Quando questo coordinamento manca, sappiamo tutti cosa potrebbe succedere. Gli amministratori desiderano seguire le loro best practice, ma, in casi disperati, aggiungono la temuta regola IP ANY/ANY ALLOW come correzione rapida per consentire agli utenti interessati di accedere a tutto, finché il problema sottostante non viene diagnosticato e risolto. Tuttavia, spesso, non c'è tempo di tornare indietro e annullare le modifiche, pertanto queste rapide correzioni diminuiscono il livello di sicurezza di un'azienda nel tempo.

Le VPN aggiungono problemi di complessità, performance e sicurezza

Per gli utenti remoti, le VPN (Virtual Private Network), di solito, forniscono l'accesso alle applicazioni on-premise gestite all'interno del perimetro, e da lì un accesso diretto con tunnel alla rete dell'azienda.

Per gestire l'accesso degli utenti alle applicazioni, le aziende spesso aggiungono software ADC (Application Delivery Controller) dedicati o utilizzano i controlli degli accessi integrati nelle loro soluzioni VPN. Il loro obiettivo è allineare le autorizzazioni di accesso alle applicazioni indipendentemente dalle posizioni in cui si trovano gli utenti. Se ad un utente viene negato l'accesso all'applicazione CRM quando si trova all'interno del perimetro, in teoria gli verrà negato anche quando si connette tramite le VPN. Anche se questo resta l'obiettivo, la mancata sincronizzazione delle autorizzazioni di accesso tra i due casi di utilizzo, nonché l'implementazione di eventuali correzioni al volo, potrebbero tradursi nel rilascio di capacità di accesso indesiderate.

Accesso alle applicazioni per collaboratori, partner e fornitori

Le aziende spesso usano le VPN anche per consentire l'accesso remoto alle applicazioni per collaboratori, aziende partner o fornitori. Ad esempio, un'azienda potrebbe consentire l'accesso ai suoi sistemi finanziari dall'esterno per far sì che i fornitori possano inviare le fatture. Consentire a terze parti di accedere alle applicazioni tramite una VPN introduce altri rischi alla sicurezza perché l'azienda non può più controllare il sistema di sicurezza dall'inizio alla fine. Se un dispositivo di terze parti con accesso tramite VPN viene violato, i criminali possono ottenere l'accesso alla rete dell'azienda.

VPN e performance

Lo stesso compromesso si verifica con le performance. Nella forma più semplice di una VPN, tutto il traffico viene reindirizzato verso l'infrastruttura del data center. Ciò può determinare un accesso alle proprietà Internet e alle applicazioni SaaS (SaaS (Software-as-a-Service) dovuto all'hairpinning, che effettivamente raddoppia la quantità di traffico.

Per superare questo impatto sulle performance, gli amministratori spesso implementano degli "split tunnel", contrassegnando gli intervalli IP che devono attraversare la VPN e quelli che devono uscire direttamente in Internet. Questa operazione può essere semplice ed efficace se si dispone di un solo perimetro interno. Tuttavia, inizia a diventare molto più complessa se si aggiungono più provider di servizi cloud privati virtuali e data center. Gli amministratori devono quindi stabilire se installare o meno gli aggregatori di VPN in ogni data center e come gestire in modo efficace gli split tunnel multipunto.

Ciò non significa che le VPN non siano un valore. Tutto il contrario. L'accesso site-to-site per l'infrastruttura di più data center è uno dei casi in cui brillano. Tuttavia, l'accesso a livello di rete non è il paradigma corretto per gli utenti che usano gli applicativi, poiché si avvale di un compromesso innaturale tra semplicità e sicurezza/performance.

I criminali vanno a nozze con l'accesso alle applicazioni basato sulla rete

Finora, ci siamo focalizzati sui rischi e sui problemi associati al fatto di concedere a tutti i dipendenti l'accesso alla rete. Tuttavia, questo approccio espone le aziende anche ad un altro rischio: i cybercriminali che sfruttano le credenziali degli utenti o una vulnerabilità della sicurezza hanno il potenziale di ottenere un accesso illimitato alla rete. Un criminale che ottiene l'accesso alla VPN tramite la violazione delle credenziali dei dipendenti, può, ad esempio, spostarsi lateralmente sulla rete per cercare, accedere e attaccare obiettivi di alto valore.

Questi approcci possono dare adito a violazioni gravissime

In teoria, gestire con sicurezza e agilità l'accesso alle applicazioni tramite questi approcci è possibile. Probabilmente state già utilizzando una loro combinazione. Il problema è che le attività necessarie per implementarle bene, gestirle e fornire la sicurezza e le performance adeguate durante il loro ciclo di vita sono spesso troppo complesse per risultare sempre corrette. In molti casi, le aziende si convincono che il semplice fatto che i dipendenti riescano ad accedere alle loro applicazioni voglia dire che tutto funziona in modo ottimale. Poi vengono prese alla sprovvista quando una correzione rapida provoca una grave violazione o peggiora le performance al punto da interrompere le attività o limitare notevolmente la produttività dei dipendenti.

Un approccio Zero Trust all'accesso alle applicazioni

Considerando le falle intrinseche agli approcci alla sicurezza del perimetro di rete e gli specifici problemi di gestione degli accessi che presentano, il nuovo modello di cybersicurezza Zero Trust offre un'alternativa migliore. Introdotto per la prima volta da Forrester Research nel 2010, è un sistema utilizzato dalle aziende per trasformare la loro infrastruttura IT, le policy di sicurezza e i processi aziendali.

Il principio alla base è piuttosto semplice, ma molto potente: l'attendibilità non è un attributo che dipende dalla posizione. Non ci si dovrebbe fidare di qualcosa semplicemente perché si trova dietro al firewall aziendale. Al contrario, ogni azione, a prescindere da dove essa si verifichi, deve essere considerata attendibile soltanto se è stata esplicitamente consentita. In definitiva, *può* accadere soltanto ciò che *deve* accadere, rimuovendo la fiducia implicita nelle operazioni non necessarie, che possono creare rischi senza apportare valore.

Tutto ciò richiede un solido meccanismo di autenticazione e autorizzazione, in modo che i sistemi non possano trasferire i dati finché non ne viene stabilita l’attendibilità. Operazioni di analisi, filtraggio e registrazione consentono inoltre di verificare i comportamenti per restare continuamente vigili riguardo a eventuali segnali che indicano violazioni di qualsiasi tipo.

Questo fondamentale cambio di prospettiva mette fine a una cospicua quantità di compromessi sulla sicurezza che hanno caratterizzato l'ultimo decennio. I criminali non possono più sfruttare i punti deboli del vostro perimetro per attaccare applicazioni e dati sensibili perché non riusciranno più a entrare nel castello. Ora non esiste più alcun fossato da attraversare per accedere. Esistono solo utenti e applicazioni, che devono autenticarsi reciprocamente e verificare l'autorizzazione prima di poter effettuare l'accesso.

Zero Trust Network Access

L'architettura ZTNA è stata costruita su questi principi per concedere un accesso sicuro a risorse e applicazioni sulla base di un solido livello di autenticazione, autorizzazione e contesto. Un'architettura ZTNA fornisce l'accesso solo alle applicazioni che servono agli utenti per svolgere il loro lavoro, non all'intera rete. Con un approccio ZTNA, non importa più dove si trovano gli utenti perché non esiste più il concetto di interno o esterno al perimetro della rete. La posizione in cui un'applicazione viene ospitata è irrilevante (se on-premise oppure nel cloud pubblico o privato) perché solo gli utenti autenticati possono accedere alle applicazioni al cui uso sono stati autorizzati.

Ad esempio, un dipendente che lavora nel reparto vendite potrà accedere solo alle applicazioni correlate al suo ruolo, non a quelle delle risorse umane o del reparto finanziario.

Come funziona l'architettura ZTNA di Akamai

Akamai Enterprise Application Access e Akamai MFA vi consentono di passare ad un'architettura ZTNA, che può risultare una fase importante e cruciale nel vostro percorso verso il modello Zero Trust.

Enterprise Application Access è un proxy basato sulle identità (IAP) nel cloud. È un servizio flessibile e adattabile con un accesso relativo a un processo decisionale granulare basato su segnali in tempo reale, come l'intelligence sulle minacce, il comportamento dei dispositivi e le informazioni sulle identità degli utenti. Akamai MFA è un servizio di autenticazione multifattore che fornisce i massimi livelli di autenticazione per garantire che un utente che richiede l'accesso sia effettivamente chi dichiara di essere.

Per iniziare, potete eseguire una piccola macchina virtuale, ossia il connettore di Enterprise Application Access dietro il firewall, ma connessa con le vostre applicazioni. Non è necessario, *né* obbligatorio, che la MV si trovi all'interno della vostra DMZ. Il suo indirizzo deve trovarsi su uno spazio IP privato e non deve essere direttamente raggiungibile da Internet. In effetti, dovrebbe essere molto simile a qualsiasi altra applicazione situata dietro il firewall.

Per supportare gli ambienti multicloud, è possibile implementare un connettore all'interno dei vostri data center on-premise oppure in un cloud pubblico o privato.

Il connettore di Enterprise Application Access stabilisce immediatamente una connessione crittografata in uscita con l'IAP su Akamai Connected Cloud. Una volta effettuata la connessione con l'IAP, il connettore esegue il download della sua configurazione per prepararsi alle connessioni del servizio. La connessione del connettore all'IAP è in uscita, ossia consente di chiudere tutte le connessioni del firewall in entrata, rendendo le applicazioni praticamente invisibili sull'Internet pubblico.

L'IAP esegue tutte le operazioni di pre-elaborazione prima di connettere un utente all'applicazione, inclusi i processi di autenticazione e autorizzazione e i controlli del comportamento e della sicurezza dei dispositivi. Quando un utente tenta di accedere ad un'applicazione, viene indirizzato ad Akamai tramite un DNS CNAME e connesso all'IAP. Supponendo che l'utente finale e il relativo dispositivo superino tutti i controlli, vengono quindi instradati per l'esecuzione della normale autenticazione, dell'autenticazione multifattore e del Single Sign-On, al termine delle quali vengono eseguite le funzioni di identità dei dispositivi.

Una volta autorizzati l'utente e il computer, la connessione da parte dell'utente finale viene unita alla connessione in uscita dal connettore di Enterprise Application Access. Il traffico dalla sessione utente scorre attraverso l'IAP unificato, che quindi si collega all'applicazione o al servizio richiesti. A questo punto, viene stabilito un percorso dati completo e tutte le decisioni relative all'accesso vengono applicate continuamente e dinamicamente in base alle identità, ai dispositivi e al contesto dell'utente.

Questo metodo di accesso presenta vantaggi distintivi e significativi. Le attività che dipendono maggiormente dalle performance e dalla sicurezza vengono svolte più vicino all'utente finale in prossimità dell'edge, su cui Akamai dispone di più di 4.200 sedi in 134 paesi.

Inoltre, il percorso di ingresso sensibile all'applicazione avviene su un tunnel di applicazioni inverso, il che rimuove efficacemente la visibilità dell'IP del perimetro e riduce il rischio di attacchi volumetrici.

Poiché Enterprise Application Access è in grado di integrarsi direttamente nell'infrastruttura delle identità di un'azienda, persino se include più directory e provider di servizi di identità, è possibile implementare rapidamente il servizio ZTNA senza la necessità di modificare l'architettura o l'infrastruttura delle identità esistente.

Per le applicazioni tradizionali che non supportano i moderni protocolli di autenticazione, Enterprise Application Access dispone di una funzionalità di collegamento IdP, che fornisce l'autenticazione agli IdP basati su SAML e converte il token di autenticazione nel protocollo supportato dalle applicazioni tradizionali.

Ciò che rende così interessanti gli approcci basati su IAP, come Enterprise Application Access, è il fatto di offrire un accesso a livello di applicazione. In questo modo, le performance e la sicurezza vengono *svincolate* dalla complessità.

È sufficiente prendere tutte le applicazioni che si trovano vicine (ad esempio, ospitate nello stesso data center o cloud privato), inserirle in uno spazio IP di una rete privata o su una VLAN limitata, posizionare un proxy di accesso in quel micro-perimetro e il gioco è fatto.

I proprietari delle applicazioni impostano le proprie policy di sicurezza (relative a chi può accedere a cosa e perché) sul proxy di accesso e, cosa ancora più interessante, gli utenti possono trovarsi ovunque. Non esiste più alcuna differenza tra gli utenti on-premise e off-premise perché non esiste alcun perimetro di rete che include gli utenti finali. Un dipendente che lavora in una caffetteria è equivalente a un dipendente che lavora in ufficio. L'unico aspetto che conta è se l'utente è autorizzato e se il computer è sicuro.

Con l'accesso a livello di applicazione, potete ottenere le migliori performance, nonostante la semplicità di implementazione e utilizzo. Gli utenti devono semplicemente utilizzare Internet per accedere direttamente alle applicazioni, indipendentemente dalle posizioni in cui sono ospitate o vengono visualizzate le applicazioni, consentendo ad Internet di instradare i pacchetti verso la loro destinazione senza dover passare per aggregatori o intermediari che non si trovano sul loro percorso.

In realtà, con l'accesso a livello di applicazione, le reti interne spesso si dissolvono in semplici Wi-Fi guest. Occorre ricordare che, affinché la rete Zero Trust sia davvero efficace, non è possibile trattare gli utenti interni in modo diverso da quelli esterni: nessun utente o dispositivo è da considerare automaticamente attendibile.

Lo stato finale desiderato dell'architettura ZTNA

Tutti gli utenti, indipendentemente dal fatto che si trovino on-premise oppure off-premise, dovrebbero essere obbligati ad accedere a tutte le applicazioni tramite i proxy di accesso basati sulle identità, indipendentemente dalla posizione in cui vengono ospitate le applicazioni. Questi proxy dovrebbero eseguire non solo l'autenticazione standard, ma utilizzare anche l'autenticazione multifattore anti-phishing, come Akamai MFA. Inoltre, dovrebbero essere disponibili funzionalità affidabili per il comportamento dei dispositivi che richiedano criteri del dispositivo per consentire l'accesso a specifiche applicazioni.

Siamo convinti che l'approccio ZTNA non termina con l'autenticazione e l'autorizzazione. Per supportare i principi Zero, tutti i parametri controllati nelle fasi iniziali di autenticazione e autorizzazione dovrebbero essere continuamente monitorati durante la sessione di attivazione. Eventuali cambiamenti rilevati dovrebbero attivare una specifica azione, ad esempio, eseguire nuovamente l'autenticazione dell'utente oppure rimuovere o limitare l'accesso all'applicazione.

Un sistema di sicurezza fondamentale sul quale dovrebbero fare affidamento i vostri proxy di accesso è una soluzione WAAP (Web Application and API Protection) per garantire che i vostri utenti finali non sferrino (intenzionalmente o inavvertitamente) attacchi alle vostre applicazioni interne. Potete sfruttare altri sistemi avanzati, come ad esempio il rilevamento di utenti umani/bot per i siti non API, per garantire che nessun malware si nasconda dietro validi endpoint. Sull'IAP, Akamai può aggiungere livelli quali WAAP, rilevamento di bot, analisi comportamentale e memorizzazione nella cache. Un simile design è progettato per fornire le migliori performance, nonché la possibilità di tenere potenziali vettori di minacce il più lontano possibile dalle vostre posizioni fisiche, applicazioni e dati.

Man mano che rendete le vostre applicazioni disponibili online e accessibili tramite i proxy di accesso, la prevenzione dagli attacchi DDOS (Distributed Denial-of-Service) diventa ancora più importante. Dovete allinearvi con provider che possono assorbire gli attacchi contro i vostri micro-perimetri e proxy di accesso, consentendo un funzionamento continuo con carichi di lavoro elevati.

Infine, per garantire che le performance delle applicazioni siano di livello eccellente e che gli utenti non solo accettino questo cambiamento di accesso, ma lo promuovano, i vostri proxy di accesso devono essere in grado di offrire vantaggi in termini di performance. In particolare, le reti per la distribuzione dei contenuti e le sovrapposizioni di instradamento Internet usati dovrebbero essere parte del vostro arsenale, non solo per rendere disponibile l'accesso, ma anche per renderlo più performante rispetto alle precedenti metodologie.

Protezione dalle minacce

Soluzioni come Akamai Enterprise Application Access possono proteggere le vostre applicazioni dai criminali. Ma come fare a impedire che gli utenti diventino inavvertitamente i vettori di una violazione, ad esempio tramite un dispositivo infettato da malware o credenziali rubate tramite un collegamento di phishing e una pagina di destinazione? È qui che la prevenzione e il rilevamento diventano cruciali per il traffico web.

Un approccio consiste nell'implementazione di una soluzione di firewall DNS basata su cloud come Akamai Secure Internet Access. Questo prodotto ispeziona ogni richiesta DNS degli utenti e applica l'intelligence sulle minacce in tempo reale in modo da risolvere le richieste legittime come normali, mentre ogni richiesta effettuata a domini dannosi viene bloccata in modo proattivo. Ciò riduce i rischi di violazione dei dispositivi dei dipendenti da parte di malware o ransomware oppure di subire un attacco di phishing.

Riepilogo

Le tradizionali architetture di rete hub e spoke, insieme al perimetro di sicurezza basato su un modello che vedeva l'organizzazione come un castello da difendere attraverso la costruzione di mura e fossati, semplicemente non possono fornire in modo efficace performance o sicurezza nel mondo cloud e mobile di oggi. Questo è un problema che tutte le aziende devono iniziare ad affrontare per evitare vulnerabilità. La mancata adozione di architetture di rete più sicure è, attualmente, la principale causa delle violazioni delle reti aziendali e il numero di questi incidenti può solo aumentare. Più semplicemente, non siete al sicuro dietro al perimetro perché il perimetro stesso non esiste più.

Passaggi successivi

In che modo è possibile iniziare il passaggio a un'architettura Zero Trust Network Access?

I servizi di sicurezza nel cloud di Akamai possono essere combinati per creare un'architettura ZTNA completa, consentendo non solo l'accesso sicuro alle applicazioni nel mondo del multicloud, ma anche l'utilizzo del cloud per rimuovere quasi completamente la necessità di reti aziendali interne.

Grazie alla nostra avanzata soluzione IAP distribuita e alla nostra autenticazione multifattore anti-phishing, insieme alla potenza di Akamai Connected Cloud, potete passare finalmente a un mondo meno perimetrale in modo semplicissimo, eseguendo il phasing delle applicazioni, azzerando quasi il profilo del rischio di migrazione e sfruttando la vasta esperienza di Akamai, che vanta soluzioni per le performance e la sicurezza di comprovata validità.

Mentre continuate il vostro percorso verso un'architettura Zero Trust, potete essere certi che Akamai vi sarà accanto in ogni fase, aiutandovi con la trasformazione della vostra rete in un'architettura che non solo garantisce l'accesso alle vostre applicazioni e ai vostri dati, ma lo fa anche in un modo facile da gestire, mantenendo i più alti livelli di sicurezza e performance.

Scoprite di più su come soddisfare le esigenze aziendali con il portfolio Zero Trust di Akamai.

A sostegno e protezione della vita online c'è sempre Akamai. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. Akamai Connected Cloud, una piattaforma edge e cloud ampiamente distribuita, avvicina le app e le experience agli utenti e allontana le minacce. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 02/24.