E-book

La guida dei CISO alla prevenzione delle minacce

Trova la soluzione migliore per proteggerti dalle minacce avanzate e basate su file.

Contenuti

Ripensare la sicurezza per l'attuale panorama di minacce

La sicurezza basata solo sul perimetro è troppo rischiosa per il mondo digitale di oggi

Il passaggio al lavoro flessibile e alle applicazioni ospitate sul cloud ha cambiato le modalità in cui gli utenti accedono alle risorse aziendali. Gli utenti utilizzano dispositivi non gestiti su reti non protette, come il Wi-Fi pubblico, per rimanere produttivi da remoto o mentre sono in viaggio; Internet è quindi diventata la nuova rete aziendale. Questo estende il perimetro di un'azienda a migliaia di entità, motivo per cui l'approccio alla sicurezza di tipo a "castello e fossato" si rivela inadeguato per proteggere utenti, applicazioni e dati. Continuare ad affidarsi solamente ai controlli perimetrali introduce dei rischi, in quanto le difese incentrate sulla rete vengono spesso aggirate per maggiore facilità d'uso e per ottenere l'accesso diretto a Internet.

Gli attacchi informatici di nuova generazione riescono a eludere con estrema facilità i controlli di sicurezza legacy. È giunto il momento di avvicinare la sicurezza agli utenti e di passare dalla protezione del perimetro alla protezione degli utenti, dei carichi di lavoro e dell'OT/IoT.

Gli aggressori stanno approfittando della corsa al cloud

I team addetti alla sicurezza si trovano quindi tra l'incudine e il martello: hanno fatto del loro meglio per adattare i controlli di sicurezza legacy al mondo mobile e cloud di oggi, ma l'inefficacia di questi strumenti ha finito per favorire gli aggressori. Le organizzazioni faticano a proteggere più edge di rete, e di conseguenza le porte vengono inavvertitamente lasciate aperte ai malware, come dimostrato dai risultati delle ricerche di Zscaler ThreatLabz:

- Gli attacchi ransomware hanno registrato **un aumento annuo dell'80%**.[1]
- Le tecniche di estorsione articolate in più passaggi sono in aumento, e i ransomware a doppia estorsione sono incrementati del **117%**.[1]
- Rispetto al 2020, nel 2021 gli attacchi di phishing **sono aumentati del 29%**.[2]
- Nel 2021, l'**85%** delle organizzazioni ha subito un attacco informatico riuscito.[3]
- Nel 2021, il **63%** delle vittime di ransomware ha pagato i riscatti, incoraggiando di conseguenza i criminali informatici a intensificare gli attacchi.[3]

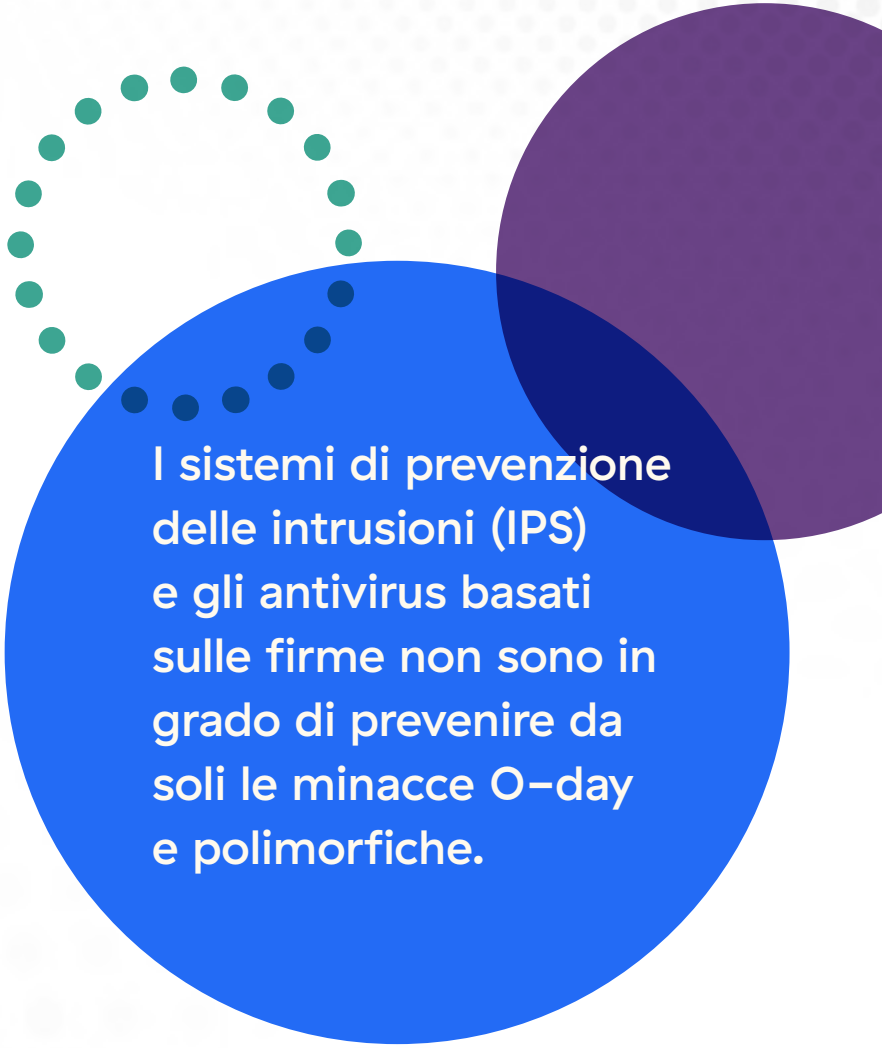
1. https://www.zscaler.it/resources/industry-reports/2022-threatlabz-ransomware-report.pdf
2. https://www.zscaler.it/resources/industry-reports/2022-threatlabz-phishing-report.pdf
3. https://cyber-edge.com/cyberthreat-defense-report-2022/

È necessario evolversi per proteggersi dai malware O-day

Gli aggressori godono di due vantaggi: **velocità** e **proliferazione**. Gli sviluppatori di malware creano minacce molto più velocemente del tempo necessario ai difensori per riconoscerle, diffondendole e modificandole per eludere il rilevamento.

Il phishing con allegati o link dannosi rimane attualmente il meccanismo di consegna più comune. Dato che le minacce si nascondono nel traffico criptato, senza ispezionare tutto il traffico web e non web, i protocolli di trasferimento dei file e il traffico SSL/TLS, si corre il rischio di far penetrare inconsapevolmente i malware nella propria rete e consentire agli aggressori di esfiltrare i dati sensibili o richiedere un riscatto.

Le sandbox hanno una funzione fondamentale in uno stack di soluzioni di sicurezza, e rappresentano una misura preventiva contro l'esecuzione di codice e file dannosi. Sono concepite per essere l'ultima linea di difesa e il primo punto di rilevamento per le indagini contro le minacce sconosciute. Purtroppo, le sandbox legacy basate su apparecchi fisici sono fuori banda e richiedono dispositivi aggiuntivi per la decrittazione e l'ispezione SSL. Inoltre, dato che la protezione viene applicata quando il malware ha già raggiunto l'utente o il dispositivo, queste soluzioni non consentono di adottare un approccio zero trust.



I requisiti di una sandbox cloud

Finora gli aggressori hanno avuto la meglio, perché hanno saputo sfruttare a loro vantaggio l'architettura mutevole dell'ambiente cloud.

Scegliere la sandbox cloud giusta è fondamentale per prevenire le infezioni da paziente zero e bloccare le minacce avanzate persistenti impedendo loro di accedere alla rete.

La sezione seguente ha lo scopo di aiutarti a comprendere i requisiti specifici da tenere in considerazione nella scelta di una sandbox cloud.

Decrittazione e ispezione su larga scala

Quella della crittografia è considerata una strategia molto promettente per garantire la sicurezza, in quanto consente di proteggere le comunicazioni private e le informazioni sensibili. Purtroppo però, anche i criminali informatici sfruttano il traffico criptato per nascondere i loro payload dannosi.

La pratica di decrittare e ispezionare il traffico è recente e richiede un'elaborazione intensiva. Le sandbox legacy, che hanno un'architettura passthrough, consentono involontariamente ai malware di insinuarsi nel traffico che non viene ispezionato. Aggiungere ulteriori dispositivi da destinare all'ispezione SSL può aiutare, ma come tutti gli apparecchi fisici, questi non sono in grado di offrire scalabilità; di conseguenza, ci si ritrova a dover gestire una moltitudine di dispositivi, e le infezioni da paziente zero continuano a penetrare nelle reti.

Quando si valuta una soluzione di sandboxing moderna, è importante capire quali sono i fornitori in grado di offrire operazioni di decrittazione e ispezione illimitate e prive di latenza.

Le minacce HTTPS hanno registrato un aumento annuo di oltre il 314%, con una crescita che ha superato il 250% per il secondo anno consecutivo.[4]

La checklist prima dell'acquisto:

- ☐ La decrittazione del traffico SSL non deve richiedere hardware aggiuntivo o l'installazione di macchine virtuali (VM)
- ☐ La soluzione deve ispezionare e analizzare i seguenti tipi di file senza latenza o limitazioni di capacità:

EXE	DOC(X)	TAR
DLL	XLX(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	File script nei file ZIP
SWF	BZ2	

4. *https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks-it*

La checklist prima dell'acquisto:

- ☐ Applicazione immediata delle policy per tutti gli utenti e con la stessa protezione, sia all'interno che all'esterno della rete aziendale
- ☐ Regole e funzionalità avanzate per la messa in quarantena di tutti i file provenienti da destinazioni sospette
- ☐ Gestione centralizzata delle policy
- ☐ Controlli granulari per i file greyware e adware

Gestione centralizzata delle policy e delle regole

Grazie alla gestione centralizzata delle policy e delle regole fornita sul cloud, puoi evitare gli errori di gestione delle regole e la configurazione manuale delle sandbox per ogni gateway. Considera le soluzioni che sfruttano policy adattive e dinamiche e che seguono i principi dello zero trust delineati nella **pubblicazione 800-207 del NIST**. Definendo policy di accesso e sicurezza basate sul contesto e includendo fattori come il ruolo e la posizione dell'utente, il profilo di sicurezza del dispositivo e i dati richiesti, lo zero trust riduce al minimo le superfici di attacco. Le soluzioni fornite sul cloud offrono anche altri vantaggi, e una volta identificata una minaccia, consentono di bloccarla per tutti gli utenti dell'organizzazione. Questo significa che è possibile migliorare la sicurezza senza dover più eseguire operazioni retrospettive sui file (come ispezioni fuori banda e l'applicazione di protezioni a posteriori).

I controlli granulari consentono di allineare le policy alla tolleranza al rischio e alle aspettative prestazionali dell'organizzazione.

Allineamento delle policy alla tolleranza al rischio e alle aspettative prestazionali

Una soluzione sandbox cloud deve controllare i rischi e applicare policy conformi alle esigenze specifiche dell'organizzazione. Inizia determinando se l'azienda ha:

- **Una bassa tolleranza ai file dannosi:** le organizzazioni con una bassa tolleranza al rischio hanno l'opzione di mettere in quarantena i file sconosciuti o sospetti scaricati per la prima volta.
- **Una bassa tolleranza alla messa in quarantena dei file:** le organizzazioni con una maggiore tolleranza al rischio che desiderano evitare ritardi e interruzioni possono scegliere di procedere all'autorizzazione e alla scansione dei file scaricati per la prima volta. Per una maggiore protezione, è possibile integrare anche funzionalità di isolamento del browser cloud, per renderizzare il file sotto forma di immagine ed evitare quindi le fughe di dati e la distribuzione di minacce attive.

Indipendentemente dalle esigenze specifiche, le policy devono essere facili da applicare a tutti gli utenti, i gruppi, i reparti, le sedi e i gruppi di sedi attraverso un'unica piattaforma.

Analisi intelligente e informazioni sulle minacce

È risaputo che gli aggressori riutilizzano gli attacchi che hanno avuto successo; per questo motivo, è essenziale condividere le protezioni utilizzate con il resto della community della sicurezza, in modo da bloccare rapidamente le minacce. Le sandbox cloud svolgono un ruolo importante in questo senso, in quanto acquisiscono i dati telemetrici e condividono le informazioni sulle minacce appena identificate con i feed e l'intera community.

Motore di prevenzione dei malware alimentato dall'IA

Le sandbox distribuite sul cloud sono in grado di gestire modelli di IA/ML a elevata intensità di calcolo, per garantire una protezione di livello superiore.

Cerca una sandbox in grado di identificare, mettere in quarantena e prevenire inline le minacce sconosciute o sospette utilizzando funzionalità avanzate basate su IA/ML ed evitando di scansionare nuovamente i file benigni.
Questo garantisce:

- **Verdetti più rapidi sui file:** grazie all'instradamento immediato dei file benigni e all'analisi dei file sospetti o sconosciuti, puoi ridurre il lavoro manuale.
- **Prevenzione delle minacce 0-day:** mettendo in quarantena le minacce sconosciute senza dover effettuare ulteriori operazioni, puoi evitare che le 0-day diventino minacce più gravi per l'ambiente aziendale.

Flussi di lavoro SOC che sfruttano l'intelligence sulle minacce

Il rilevamento di una singola minaccia può richiedere molte ore di lavoro per gli analisti. Per questo, cerca una sandbox cloud che riduca questo carico e consenta di accelerare le azioni di indagine e risposta condividendo le informazioni sul comportamento e l'intelligence sui payload dannosi. Assicurati che i feed sulle minacce si integrino con gli strumenti di sicurezza esistenti e che includano: contesto aggiornato sugli URL segnalati, indicatori di compromissione estratti (IoC) e tattiche, tecniche e procedure (TTP) in linea con i framework di sicurezza informatica, come MITRE ATT&CK®.

La checklist prima dell'acquisto:

- ☐ Funzionalità di ML/IA che si integrano strettamente con il processo di analisi
- ☐ Funzionalità di quarantena basate sull'IA in grado di sfruttare ML/IA per trattenere i file potenzialmente dannosi, analizzarli ed emettere verdetti rapidamente
- ☐ Contributo autonomo alle pratiche di protezione giornaliera dalle minacce condiviso tra utenti e reti, indipendentemente dalla posizione
- ☐ Possibilità di condividere i dati forensi e i verdetti sui file attraverso un sola piattaforma
- ☐ Integrazione dei feed sulle minacce con gli strumenti di sicurezza esistenti

Assicurati di scegliere una sandbox che non fornisca semplicemente un punteggio sulle minacce, ma che sia in grado di delineare le tecniche elusive utilizzate, ad esempio:

- Ritardo di esecuzione del codice per evitare il rilevamento da parte della sandbox
- Acquisizione e visualizzazione del traffico che si muove attraverso la rete
- Apertura di porte per consentire la connettività da remoto
- Tentativo di movimento laterale per individuare gli obiettivi di maggior valore
- Tentativo di consentire il controllo da remoto

Reportistica

Le soluzioni di sicurezza con funzionalità di reportistica sono utili solo se le informazioni riportate possono essere sfruttate a proprio vantaggio. La reportistica delle sandbox cloud dovrebbe:

- Comprendere l'intero ciclo di vita dell'attacco dannoso
- Essere semplice da usare e facile da consultare
- Essere facile da integrare
- Essere disponibile attraverso un'interfaccia di programmazione delle applicazioni (API), in modo da poter essere correlata ai log esistenti
- Fare parte di una piattaforma più ampia, che supporti anche la reportistica sulla conformità

Miglioramento del SOC con il framework MITRE ATT&CK

Quando si valutano le funzionalità di reportistica, è fondamentale che l'intelligence della sandbox possa essere mappata sulla base del **framework MITRE ATT&CK**. Grazie a questa funzione, i team SOC possono impiegare le informazioni ottenute per creare tattiche di difesa da applicare in altre parti dello stack di soluzioni di sicurezza. In questo modo, la sandbox diventa parte integrante dei flussi di lavoro delle operazioni di sicurezza.

A seconda della dimestichezza dell'azienda con questo framework, i report possono essere utilizzati in diversi modi:

- Ridurre le operazioni di classificazione utilizzando la tassonomia fornita
- Visualizzare le tecniche stealth che potrebbero riuscire a eludere la soluzione di rilevazione e risposta degli endpoint (EDR) adottata
- Confrontare e contrastare altri controlli
- Concentrarsi sulle TTP più comuni messe in atto contro l'organizzazione, invece di prevenire inutilmente ogni tipo di tattica e tecnica
- Eseguire un report di reverse engineering

Domande da porre prima dell'acquisto

Per aiutarti durante il processo decisionale, ecco un riepilogo delle domande principali da porre e il motivo per cui dovresti porle:

La soluzione copre tutti gli utenti e i loro dispositivi, indipendentemente dalla posizione?
È possibile che gli utenti accedano alle risorse aziendali quando sono in viaggio, con i propri dispositivi personali o tramite reti non protette. È fondamentale dunque proteggere tutti i dispositivi necessari ai dipendenti per portare a termine il lavoro.[5]

La soluzione funziona inline o in modalità TAP (Test Access Point)?
Le soluzioni che funzionano inline sono in grado di identificare le minacce e bloccarle direttamente, senza che sia necessario creare nuove regole tramite dispositivi terzi, come i firewall.

La sandbox esamina il traffico di tutti i protocolli HTTP, HTTPS, FTP e FTP su HTTP? Ci sono delle limitazioni?
È importante esaminare il traffico per riuscire a smascherare le minacce nascoste. Una sandbox distribuita sul cloud potrebbe essere la soluzione migliore per ispezionare tutto il traffico senza latenza.

È conforme alle leggi, alle normative vigenti e ai requisiti zero trust?
Le normative sulla conformità possono prevedere requisiti molto rigorosi sulla modalità di gestione delle sandbox e sulla conservazione/privacy dei file. Una soluzione che opera solo su memoria ed elimina le informazioni di identificazione durante l'analisi aiuta a soddisfare questi requisiti. Inoltre, è opportuno valutare l'aderenza ai principi dello zero trust definiti dagli standard globali della pubblicazione 800-207 del NIST e l'utilizzo di questi ultimi come linea guida per ridurre le superfici di attacco e proteggere i dati.

Con quali altri moduli di sicurezza funziona la sandbox?
I prodotti singoli e isolati non sono in grado di fornire una protezione completa dalle minacce avanzate persistenti (APT). È invece necessario un approccio multilivello di prevenzione, mitigazione, rilevamento e risposta alle minacce. La sandbox rappresenta un livello essenziale e, come tale, deve funzionare in modo efficiente con altre soluzioni e moduli.

La soluzione è complementare alle sandbox fornite dal provider o alle sandbox EDR?
Una vera strategia di difesa avanzata potrebbe richiedere soluzioni complementari e una protezione a più livelli per contrastare in modo adeguato la kill chain del malware che potrebbe devastare l'organizzazione. In questo modo, se un livello dell'ecosistema fallisce, si può sempre contare sul successivo e garantire la protezione. Endpoint, rete e controllo delle policy dovrebbero operare insieme in modo armonico per bloccare gli aggressori.

5. https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox e Advanced Threat Protection

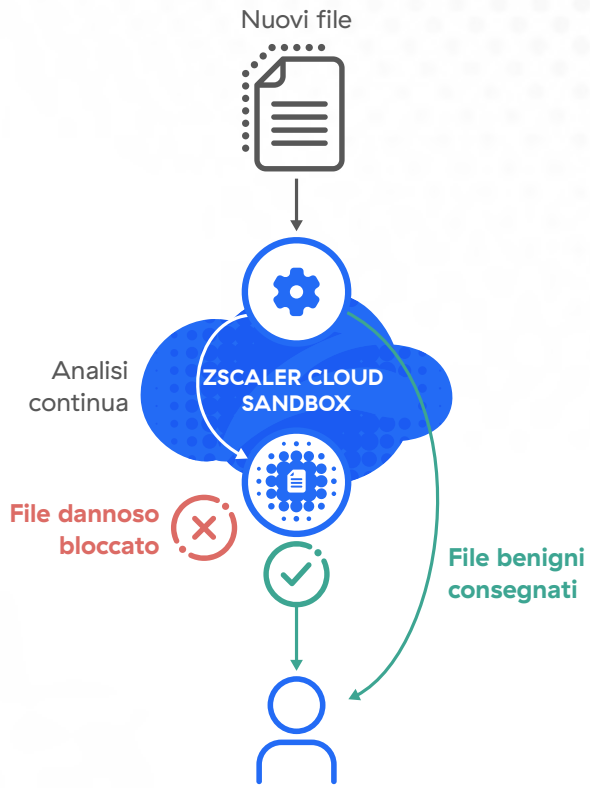
È tempo di usare una vera sandbox inline e nativa del cloud

Le organizzazioni sono alle prese con superfici di attacco sempre più estese, e gli aggressori sfruttano le lacune negli stack di soluzioni di sicurezza legacy; per questo motivo, è giunto il momento di scegliere una vera sandbox inline e nativa del cloud. Zscaler Cloud Sandbox è una soluzione creata appositamente per catturare e bloccare le minacce moderne e garantire al contempo la protezione contro i malware O-day per tutti gli utenti e in ogni luogo.

Zscaler Cloud Sandbox si fonda su un'architettura nativa del cloud e basata su proxy, ed è il primo motore di prevenzione dei malware basato su IA del mondo, in grado di rilevare, prevenire e mettere in quarantena in modo automatico e intelligente le minacce sconosciute e i file sospetti inline. L'ispezione illimitata e senza latenza di tutti i protocolli di trasferimento di file (FTP) e web, inclusi SSL e TLS, consente alla sandbox cloud di eseguire un'analisi dinamica approfondita e in tempo reale, per garantire che nessun file sconosciuto raggiunga l'utente e impedire quindi il download dei file dannosi.

La quarantena basata sull'IA blocca i malware sconosciuti

Protezione inline con consegna istantanea dei file benigni, difesa da paziente zero e controlli granulari delle policy



Riduzione di complessità e costi

- Facile da distribuire, senza hardware o software da gestire
- Eliminazione dei prodotti ridondanti e isolati
- Eliminazione del backhauling del traffico Internet su MPLS o VPN

Protezione immediata e adattiva di tutti gli utenti e le sedi

- Definizione globale delle policy tramite un'unica console centralizzata
- Applicazione immediata delle policy aggiornate
- Identificazione delle minacce una sola volta e blocco immediato per proteggere tutti i clienti

Rilevamento delle minacce nascoste

- Blocco delle infezioni da paziente zero provenienti da minacce note ed emergenti con la quarantena basata sull'IA
- Upload dei file per l'analisi (portale filecheck)

Una piattaforma integrata fornita come servizio

- Filtraggio preliminare di tutte le minacce dannose note tramite antivirus, liste di blocco degli hash, regole YARA per la classificazione dei malware, rilevamento automatico delle impronte digitali JA3 e modelli di ML/IA
- I feed del CIF (Collective Intelligence Framework) consentono a Zscaler di integrarsi con oltre 60 feed sulle minacce che si aggiungono al feed di Zscaler e di sfruttare miliardi di transazioni all'interno del suo bacino di clienti.
- Una protezione multilivello che abbina una sandbox cloud a una soluzione EDR consente di migliorare l'efficacia della sicurezza e mitigare l'accesso iniziale, l'esecuzione e le tattiche persistenti

Uno studio condotto da ESG Economic Validation ha rivelato che Zscaler Zero Trust Exchange ha consentito di ridurre del 90% il numero dei dispositivi di sicurezza.[6]

- Analisi statica, dinamica e secondaria, che include l'analisi del codice e dei payload secondari
- Ispezione SSL illimitata e senza latenza
- Protezione del traffico in entrata e in uscita
- Miglioramento delle indagini di sicurezza e delle azioni di risposta grazie a una ricca documentazione forense che include utenti, origine della posizione, tattiche elusive e altro ancora

Zscaler Cloud Sandbox è una funzionalità completamente integrata in Zscaler Internet Access e che fa parte di Zero Trust Exchange.

Per ulteriori informazioni, visita **zscaler.it/custom-product-demo.**

6. https://info.zscaler.com/resources-industry-report-esg-economic-validation-it

Experience your world, secured.™

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata su SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.it