Whitepaper sul modello di maturità Zero Trust della CISA

©2025 Zscaler, Inc. Tutti i diritti riservati.

WHITE PAPER

Riepilogo

Nell'attuale panorama in rapida evoluzione della sicurezza informatica, le organizzazioni si trovano ad affrontare una gamma crescente di minacce sofisticate. Poiché la trasformazione digitale accelera, e lavorare da qualsiasi luogo è ormai la norma, i modelli di sicurezza tradizionali basati sul perimetro sono sempre più inefficaci nel proteggere le reti. La sicurezza informatica deve evolversi per proteggere dati e sistemi, indipendentemente da dove si trovino gli utenti o i dispositivi. In risposta a queste sfide, la Cybersecurity and Infrastructure Security Agency (CISA) ha sviluppato un modello di maturità Zero Trust per guidare le organizzazioni nell'adozione e nell'implementazione efficace dei principi dello zero trust.

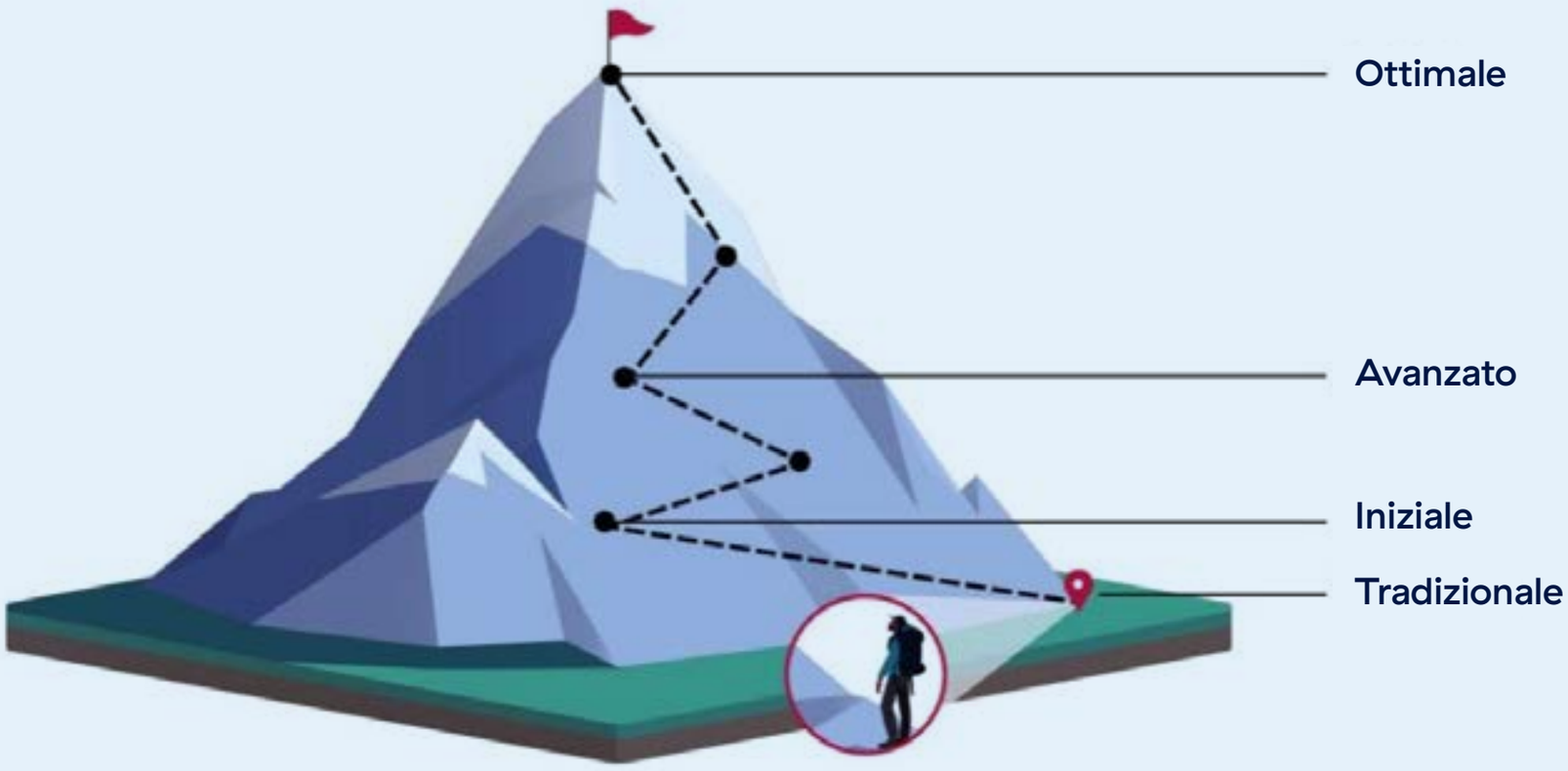
Cosa si intende per zero trust?

Lo zero trust è un modello di sicurezza basato sul presupposto che le minacce possono essere interne o esterne, quindi nessun utente o dispositivo dovrebbe essere considerato automaticamente attendibile. Ogni richiesta di accesso proveniente dall'interno o dall'esterno della rete viene rigorosamente autenticata, autorizzata e costantemente monitorata. Il framework dello zero trust ha l'obiettivo di garantire che la sicurezza sia mantenuta nell'intera infrastruttura di un'organizzazione, con particolare attenzione all'identità, alla gestione degli accessi e al monitoraggio in tempo reale.

Che cos'è il modello di maturità Zero Trust della CISA?

Il modello di maturità Zero Trust della CISA fornisce alle organizzazioni un quadro per un'adozione graduale e strutturata dei principi dello zero trust. Questo modello delinea un approccio graduale all'implementazione dello zero trust all'interno di un'organizzazione, partendo dalla fase iniziale di consapevolezza e pianificazione fino a raggiungere operazioni di sicurezza pienamente mature e integrate. Per farlo, fornisce un metodo strutturato per comprendere a che punto si trova un'organizzazione nel suo percorso verso lo zero trust e quali passaggi dovrebbe intraprendere per migliorare la sicurezza.

Percorso verso la maturità dello zero trust



Fonte: CISA

©2025 Zscaler, Inc. Tutti i diritti riservati.

Il modello CISA suddivide Zero Trust in diverse aree chiave, tra cui la gestione dell'identità e dell'accesso, la sicurezza dei dispositivi, la sicurezza della rete, la sicurezza dei dati, la sicurezza delle applicazioni, nonché la visibilità e l'analisi. Il modello di maturità aiuta le organizzazioni a valutare le proprie capacità attuali in ciascuna di queste aree e a definire un percorso chiaro per rafforzare il proprio profilo di sicurezza. Le organizzazioni vengono valutate in base a quattro livelli di maturità (tradizionale, iniziale, avanzata e ottimale), ciascuno dei quali richiede un livello di protezione maggiore, con una crescita esponenziale di attività mirate e benefici.

Il modello di maturità Zero Trust della CISA viene sempre più utilizzato come punto di riferimento globale per l'implementazione di Zero Trust. I governi internazionali, tra cui Regno Unito e Australia, hanno allineato le proprie strategie di sicurezza informatica a questo modello di maturità, riconoscendo i vantaggi di questo approccio per il miglioramento delle capacità zero trust. Oltre ai governi, la Cloud Security Alliance ha anche mappato il suo Zero Trust Advancement Center sul questo modello di maturità, rafforzando ulteriormente il suo ruolo di quadro comune per le organizzazioni di tutto il mondo. Con la crescente adozione dello zero trust, il modello di maturità fornisce un linguaggio condiviso e una roadmap di sviluppo, aiutando le entità del settore pubblico e privato a valutare i propri progressi e a perfezionare le proprie strategie di sicurezza.

I COMPONENTI PRINCIPALI DEL MODELLO

1. **Gestione dell'identità e degli accessi (IAM):** stabilisce meccanismi di autenticazione avanzati, come l'autenticazione a più fattori (MFA), per verificare l'identità degli utenti prima di concedere l'accesso.

2. **Sicurezza dei dispositivi:** garantisce che i dispositivi siano sicuri, gestiti e conformi alle policy di sicurezza prima di accedere alle risorse aziendali.

3. **Sicurezza di rete:** implementa la segmentazione e il monitoraggio per limitare il movimento laterale e rilevare attività sospette all'interno della rete.

4. **Sicurezza dei dati:** protegge i dati sensibili applicando la crittografia, rigorosi controlli di accesso e monitorando l'utilizzo dei dati.

5. **Sicurezza delle applicazioni:** garantisce la sicurezza delle applicazioni implementando pratiche di sviluppo sicure, monitoraggio continuo e gestione delle vulnerabilità.

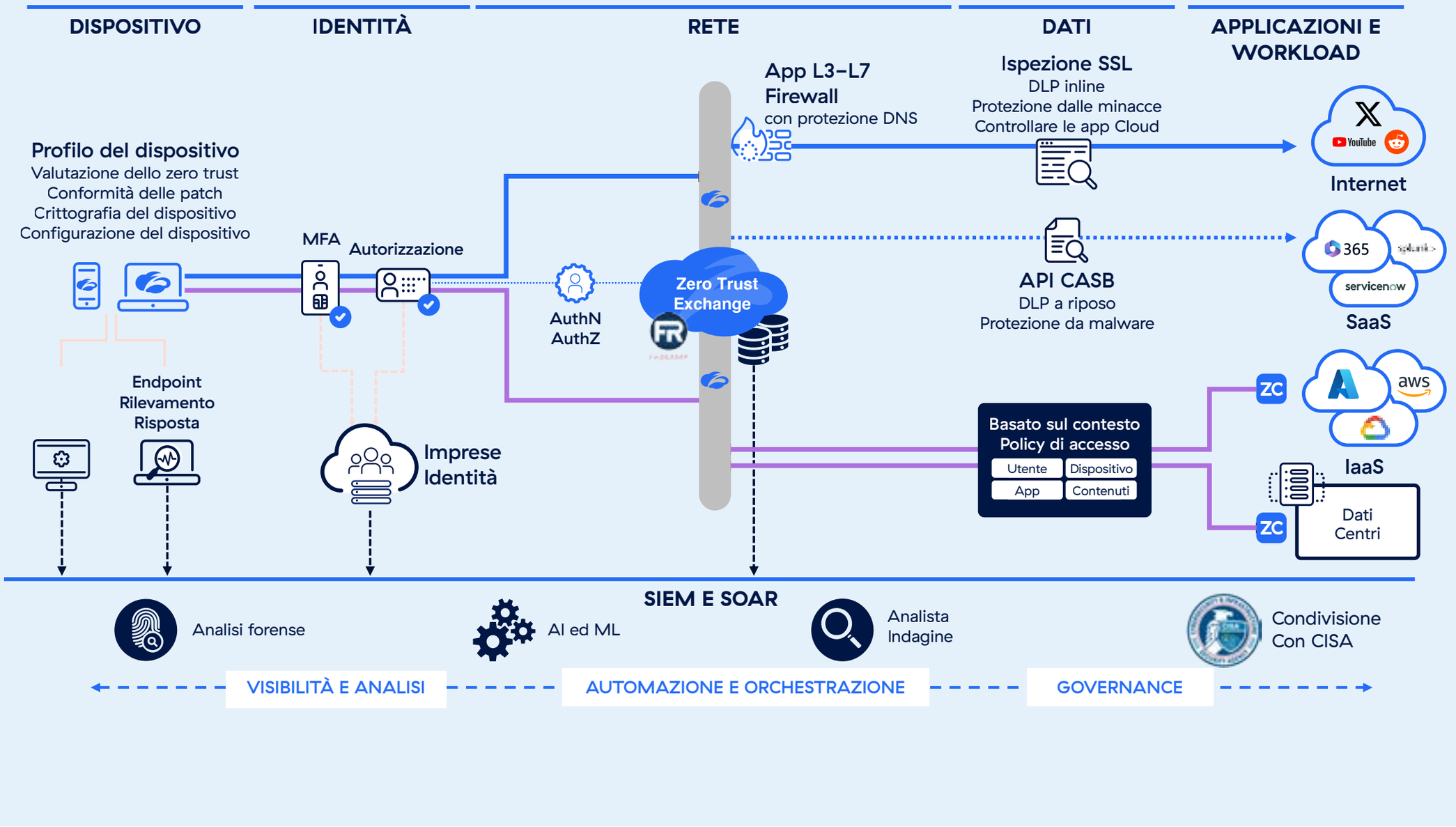
6. **Visibilità e analisi:** migliora la consapevolezza della situazione monitorando costantemente tutto il traffico e gli eventi, identificando comportamenti anomali e fornendo avvisi in tempo reale.

7. **Automazione e orchestrazione:** integra e automatizza i sistemi per migliorare l'efficacia e l'efficienza dei sistemi informatici.

8. **Governance:** stabilisce policy, procedure e meccanismi di supervisione per garantire un'attuazione efficace.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Modello di maturità Zero Trust 2.0 della CISA



Implementazione del modello di maturità Zero Trust della CISA con Zscaler

L'implementazione di Zscaler ZTE migliora immediatamente la tua sicurezza, consentendoti di passare dalla tradizionale sicurezza perimetrale a una difesa più completa e stratificata. Verificando costantemente utenti, dispositivi e dati, le organizzazioni possono ridurre il rischio di violazioni dei dati, minacce interne e attacchi esterni. Questo approccio riduce al minimo la superficie di attacco e impedisce il movimento laterale degli aggressori. Zscaler consente inoltre alle organizzazioni di far avanzare la propria strategia verso il modello di maturità della CISA grazie a prodotti e funzionalità affidabili che supportano aree chiave, tra cui la gestione di identità e accessi, la sicurezza di dispositivi, rete, dati e applicazioni e la visibilità e l'analisi.

IDENTITÀ

- **Accesso con privilegi minimi:** Zscaler riduce al minimo gli account con autorizzazioni eccessive applicando controlli di accesso granulari basati sui ruoli (RBAC) e policy contestuali (ad esempio, posizione dell'utente, profilo del dispositivo).

- **Single Sign-On (SSO) e autenticazione a più fattori (MFA):** le policy zero trust sono rafforzate con l'integrazione di SSO/MFA, garantendo un'autenticazione solida e riducendo il rischio di compromissione delle credenziali.

©2025 Zscaler, Inc. Tutti i diritti riservati.

- **Monitoraggio continuo degli utenti:** ZTE garantisce che gli utenti siano costantemente autenticati e che il loro comportamento sia monitorato per ridurre i rischi.

- **Integrazione con i provider di identità (IdP):** Zscaler si integra perfettamente con i principali provider di identità come Okta, Microsoft Azure AD e Ping Identity per applicare criteri di autenticazione e autorizzazione rigorosi degli utenti.

DISPOSITIVI

- **Controlli dello stato del dispositivo:** Zscaler utilizza integrazioni con strumenti di rilevamento e risposta degli endpoint (EDR) per eseguire controlli dello stato e garantire che solo i dispositivi sicuri e gestiti possano accedere alle risorse sensibili.

- **Applicazione basata su agente:** l'agente software leggero Zscaler Client Connector (ZCC) di Zscaler garantisce che tutto il traffico utente venga instradato attraverso il cloud di sicurezza Zscaler, consentendo visibilità e applicazione coerente delle policy di sicurezza.

- **Zero Trust per IoT/Unmanaged Dispositivi:** le soluzioni Zscaler includono funzionalità per controllare l'accesso da parte di dispositivi non gestiti, tra cui quelli dell'IoT, utilizzando criteri comportamentali e controlli di accesso granulari.

RETE

- **Zero Trust Network Access (ZTNA):** Zscaler Private Access (ZPA) sostituisce le VPN tradizionali con lo ZTNA. Agli utenti viene concesso l'accesso "con privilegi minimi" a specifiche applicazioni, non all'intera rete.

- **Secure Access Service Edge (SASE):** Zscaler soddisfa i requisiti dell'architettura SASE offrendo servizi di sicurezza scalabili, come Secure Web Gateway (SWG) e Cloud Firewall, in ambienti distribuiti.

- **Microsegmentazione:** Zscaler garantisce che gli utenti e i workload vengano segmentati a livello di applicazione, riducendo al minimo i movimenti laterali in caso di violazione.

- **Monitoraggio della crittografia end-to-end:** Zscaler ispeziona il traffico Internet cifrato tramite l'intercettazione SSL/TLS senza compromettere le prestazioni o la privacy.

APPLICAZIONI E WORKLOAD

- **Segmentazione delle applicazioni:** Zscaler ZPA offre una segmentazione basata sulle applicazioni anziché la tradizionale segmentazione di rete, consentendo connessioni dirette e sicure tra utente e applicazione.

- **Sicurezza del carico di lavoro:** Zscaler Workload Segmentation (ZWS) protegge le comunicazioni tra workload negli ambienti cloud pubblici e privati garantendo una "microsegmentazione basata sull'identità".

- **Monitoraggio continuo:** il monitoraggio a livello di applicazione tiene traccia delle attività degli utenti e dei modelli di accesso per individuare anomalie, assicurando che gli account compromessi non possano aumentare i propri privilegi.

- **Sicurezza SaaS:** Cloud Access Security Broker (CASB) di Zscaler controlla l'accesso alle applicazioni SaaS autorizzate e non autorizzate, impedendo l'accesso e l'utilizzo non autorizzati dei dati.

©2025 Zscaler, Inc. Tutti i diritti riservati.

DATI

- **Prevenzione della perdita di dati (DLP):** la tecnologia DLP basata su cloud di Zscaler aiuta a proteggere i dati sensibili su e-mail, web, SaaS e applicazioni private. Identifica e previene l'esfiltrazione di proprietà intellettuale (IP) e informazioni personali identificabili (PII).

- **Cloud Security Posture Management (CSPM):** Zscaler fornisce informazioni e soluzioni per le configurazioni errate nei sistemi di archiviazione cloud dei dati, riducendo il rischio di esposizione.

- **Controllo della crittografia:** Zscaler applica rigidi protocolli di crittografia sia per i dati in transito che per quelli inattivi, garantendo la protezione completa delle informazioni sensibili.

- **Rilevamento dello Shadow IT:** Zscaler CASB identifica e limita l'uso di app/servizi non approvati o ad alto rischio, proteggendo così i dati dalla perdita accidentale o dall'uso improprio dannoso.

GOVERNANCE, VISIBILITÀ E ANALISI, AUTOMAZIONE E ORCHESTRAZIONE

- **Gestione centralizzata della sicurezza:** Zscaler Zero Trust Exchange offre una visione centralizzata del traffico, delle policy e degli incidenti di sicurezza.

- **Analisi di sicurezza integrata:** Zscaler fornisce visibilità in tempo reale sull'attività degli utenti e delle applicazioni tramite dashboard e registri avanzati, integrandosi con piattaforme SIEM/SOAR per una risposta semplificata agli incidenti.

- **Threat Intelligence:** Zscaler sfrutta l'intelligence sulle minacce globali e l'analisi del comportamento per rilevare e rispondere in modo proattivo alle minacce nell'intera struttura ZT.

- **Applicazione delle policy:** Zscaler automatizza le modifiche alle policy e i controlli di conformità, garantendo una governance coerente tra utenti, app e dati.

L'approccio di implementazione dello ZT di Zscaler e il modello di maturità della CISA sono molto simili e allineati in diverse aree fondamentali, non solo relativamente ai pilastri dello zero trust. L'architettura di Zscaler supporta le principali funzioni del modello di maturità zero trust, come l'applicazione dinamica delle policy, la visibilità centralizzata e i controlli di accesso adattivi basati sul rischio, tutti elementi essenziali per lo sviluppo di una strategia zero trust. Grazie a un approccio inline nativo del cloud, Zscaler aiuta le organizzazioni a migliorare i livelli di maturità delineati nel modello della CISA, riducendo le superfici di attacco e semplificando al contempo l'accesso sicuro.

Roadmap strategica per l'adozione dello zero trust

Sia l'implementazione di Zscaler che il modello di maturità Zero Trust della CISA offrono una roadmap strategica che le organizzazioni possono seguire durante l'adozione dei principi zero trust. Suddividiamo il processo di implementazione in fasi gestibili, consentendo alle organizzazioni di stabilire obiettivi e tempi realistici per ogni fase. Questa roadmap garantisce alle organizzazioni un approccio strutturato all'implementazione dello zero trust, riducendo il rischio di lacune o passi falsi.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Implementazione incrementale

L'implementazione incrementale consente alle organizzazioni di migliorare gradualmente le proprie capacità zero trust nel tempo. Questo approccio graduale semplifica l'implementazione dello zero trust senza sovraccaricare i sistemi o le risorse esistenti. Permette inoltre alle organizzazioni di monitorare i progressi e di adattare le strategie secondo necessità. Ciò consente a Zscaler di rilasciare continuamente nuovi prodotti per migliorare la sicurezza dei nostri clienti, ma consentirà anche alla CISA di avanzare gli obiettivi nel futuro. Ciò che oggi è considerato "ottimale" potrebbe essere "avanzato" in futuro.

Nessuna organizzazione è uguale all'altra

Le esigenze e le infrastrutture di sicurezza informatica di ogni organizzazione sono uniche. L'implementazione ZTE di Zscaler e il modello di maturità Zero Trust della CISA sono sufficientemente flessibili da poter essere personalizzati in base agli obiettivi, alle sfide e alle risorse specifiche di un'organizzazione. Indipendentemente dal fatto che un'organizzazione abbia adottato completamente lo zero trust o abbia appena iniziato il suo percorso, il modello fornisce le indicazioni necessarie per adattare il framework alle proprie esigenze.

Misurazione del progresso e del successo

Il modello di maturità include parametri e criteri di valutazione chiari, che consentono alle organizzazioni di monitorare i propri progressi nel tempo. Misurando il successo rispetto a determinate fasi, le organizzazioni possono identificare le aree di miglioramento e assicurarsi di procedere nella giusta direzione per raggiungere un ambiente zero trust maturo.

Conclusione

Il modello di maturità 2.0 dello Zero Trust formulato dalla CISA fornisce alle organizzazioni un quadro chiaro e strutturato per adottare e promuovere i principi dello zero trust. Implementando questo modello, le organizzazioni possono migliorare significativamente la propria sicurezza informatica, mitigare i rischi e garantire la conformità ai requisiti normativi.

Con la continua evoluzione del panorama delle minacce, l'importanza dello zero trust non potrà che aumentare, e per questo motivo il modello della CISA sarà uno strumento fondamentale per le organizzazioni che avranno l'obiettivo di proteggere i propri ambienti digitali dalle minacce avanzate moderne. Attraverso un'implementazione strategica e incrementale, le organizzazioni possono adottare lo zero trust in un modo che si adatti alle loro esigenze e capacità specifiche, garantendo il successo a lungo termine nel loro percorso di sicurezza informatica.

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler.**

© 2025 Zscaler, Inc. Tutti i diritti riservati. Zscaler™ e gli altri marchi commerciali presenti su **zscaler.it/legal/trademarks** sono (I) marchi commerciali o marchi di servizio registrati o (II) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi commerciali sono di proprietà dei rispettivi titolari.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/it**

zscaler™

Zero Trust Everywhere