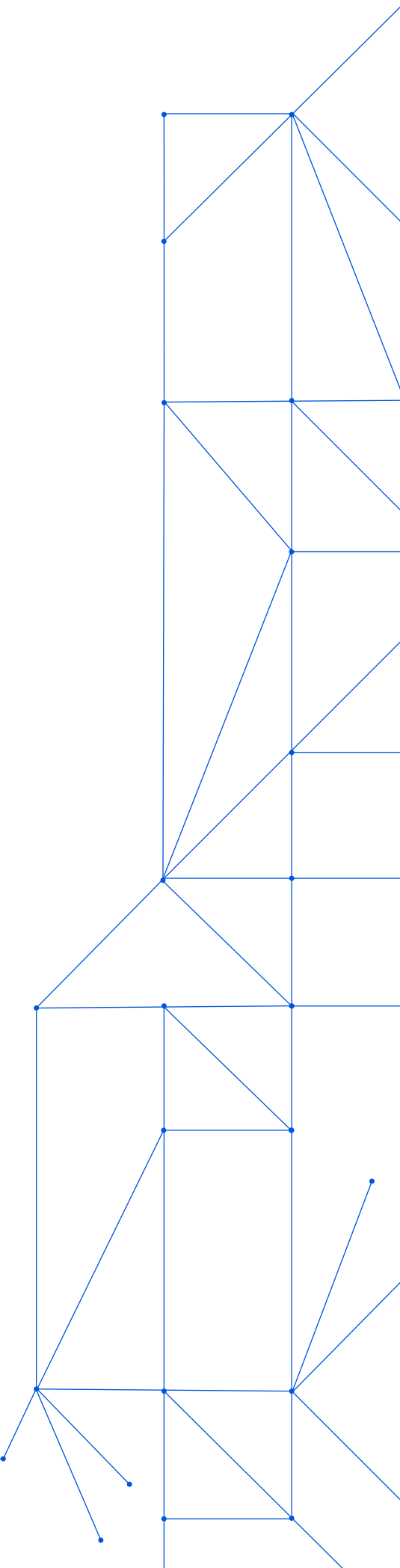
CLOUDFLARE

WHITEPAPER

Una roadmap verso l'architettura Zero Trust

Scopri i passaggi, gli strumenti e i team necessari per trasformare la tua rete e modernizzare la tua sicurezza

Contenuto



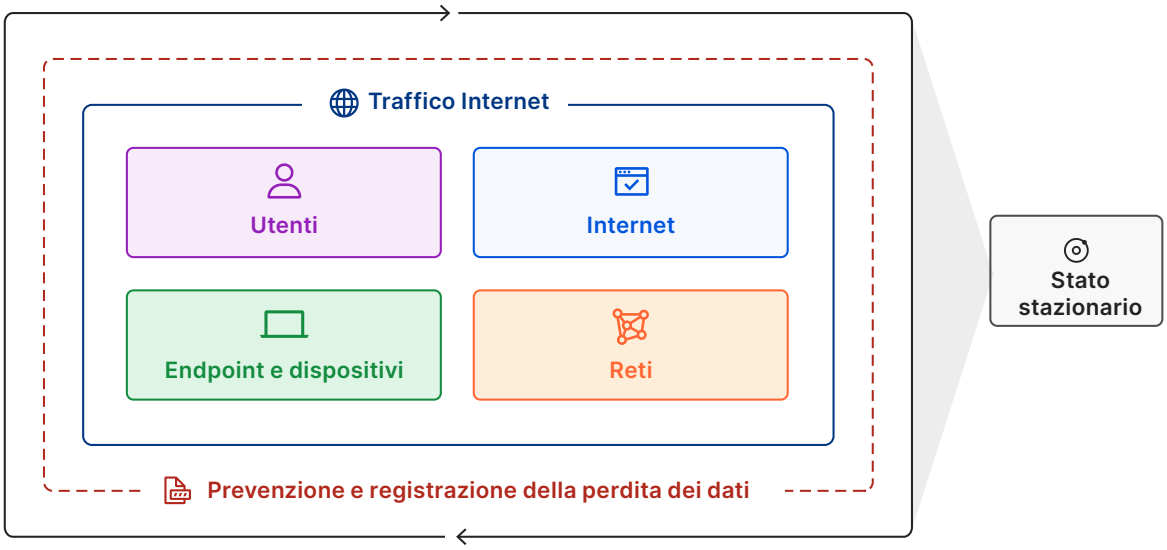
Introduzione

L'architettura di rete tradizionale è stata costruita con il concetto di una rete perimetrale in cui nel momento esatto che qualcuno era sulla rete, c'era un livello di fiducia implicito. Il passaggio all'hosting cloud, al lavoro remoto e ad altre modernizzazioni ha creato sfide con un'architettura di rete perimetrale tradizionale.

Questi problemi possono essere affrontati implementando un'architettura Zero Trust, che garantisce che tutto il traffico in entrata e in uscita da un'azienda sia verificato e autorizzato. L'implementazione di un'architettura Zero Trust può essere eseguita in più fasi senza interrompere la produttività e la connettività dei dipendenti.

Questa guida è stata creata da esperti di sicurezza per fornire un'architettura Zero Trust indipendente dal fornitore e una sequenza temporale di implementazione di esempio. La sequenza temporale presuppone che un'organizzazione stia iniziando il proprio viaggio Zero Trust da zero, ma è pensata per essere utile per tutte le organizzazioni.

Ci sono sette componenti principali per la sicurezza dell'organizzazione che devono essere considerati quando si tratta di implementare un'architettura Zero Trust completa. Non è necessario che l'ordine di implementazione corrisponda a come è riportata nelle sezioni dei componenti e dell'architettura di riferimento di seguito.



Componenti di un'architettura Zero Trust

	Componente		Scopo	Livello di sforzo	Pagina
Fase 1		traffico Internet	Distribuzione del filtraggio DNS globale	▮	9
		Internet	Monitoraggio delle e-mail in entrata ed esclusione dei tentativi di phishing	▮	13
		DLP e log	Identificazione di una configurazione errata e dei dati condivisi pubblicamente negli strumenti SaaS	▮	20
Fase 2		Utenti	Definizione dell'identità aziendale	▮▮	5
		Utenti	Applicazione dell'autenticazione a più fattori di base per tutte le applicazioni	▮	6
		Internet	Applicazione di HTTPS e DNSsec	▮	17
		traffico Internet	Blocco o isolamento delle minacce dietro SSL	▮▮	9-10
		Internet	Applicazione dei criteri ZT per le app indirizzabili pubblicamente	▮	14-16
		Internet	Protezione delle applicazioni dagli attacchi di livello 7	▮	16
		Reti	Chiusura di tutte le porte in entrata aperte su Internet per la consegna delle app	▮	12
La Fase 3		Internet	Inventario di tutte le applicazioni aziendali	▮▮	13-14
		Internet	Applicazione dei criteri ZT per le applicazioni SaaS	▮▮	14-16
		Reti	Segmentazione dell'accesso alla rete dell'utente	▮▮▮	11
		Internet	ZTNA per applicazioni critiche indirizzabili privatamente	▮	14-16
		Dispositivi	Implementazione di MDM/UEM per controllare i dispositivi aziendali	▮▮	7
		DLP e log	Definizione dei dati sensibili e di dove si trovano	▮▮	18-19
		Utenti	Invio di token di autenticazione basati su hardware	▮▮	6
		DLP e log	Rimanere aggiornati sui soggetti noti delle minacce	▮	21
Fase 4		Utenti	Applicazione dell'autenticazione a più fattori basata su token hardware	▮▮	6
		Internet	Applicazione dei criteri ZT e accesso alla rete per tutte le applicazioni	▮▮▮	14-16
		DLP e log	Definizione di un SOC per la revisione dei log, gli aggiornamenti dei criteri e la mitigazione	▮▮	20
		Dispositivi	Implementazione della protezione degli endpoint	▮▮	7
		Dispositivi	Inventario di tutti i dispositivi, le API e i servizi aziendali	▮	8
		Reti	Utilizzo di Internet a banda larga per la connettività tra filiali	▮▮▮	11-12
		DLP e log	Registrazione e revisione dell'attività dei dipendenti su app sensibili	▮▮	18
		DLP e log	Impedire ai dati sensibili di lasciare le tue applicazioni	▮▮▮	19
		Stato stazionario	Approccio DevOps per l'applicazione dei criteri di nuove risorse	▮▮	22
		Stato stazionario	Implementazione della scalabilità automatica per le risorse on-ramp	▮▮▮	22-23

Ecco come definiamo i diversi livelli di sforzo richiesti per ogni fase:

- ▮ - **Piccolo sforzo: questa fase può essere completata da un singolo individuo o da un piccolo team**
- ▮▮ - **Sforzo medio:** questa fase richiede una squadra e una preparazione avanzata
- ▮▮▮ - **Grande sforzo:** questa fase richiederà più team e un piano di progetto

La strada verso Zero Trust

Utenti

Per utenti si intendono dipendenti, appaltatori e clienti. Per implementare Zero Trust, un'organizzazione deve prima avere un quadro accurato di chi è effettivamente attendibile e con cosa, ovvero l'identità dei singoli utenti, quindi deve stabilire un modo per autenticare in modo sicuro questa identità.

Definizione di una identità aziendale

Livello di sforzo	- **Sforzo medio**
Team interessati	• Il team responsabile per il tuo provider di identità (di solito il team di sicurezza o IT) • Gli amministratori che gestiscono le app interne utilizzate da dipendenti e partner
Prodotti	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
Riepilogo	Per autenticare e autorizzare con precisione l'accesso degli utenti alle applicazioni aziendali, è necessaria un'identità aziendale unificata. Un'identità aziendale coerente renderà l'applicazione dettagliata dei criteri per le tue applicazioni più fluida. **Altri punti da considerare:** • La tua azienda è attiva in M&A? Come consoliderai gli archivi di identità? • Sono in uso protocolli di autenticazione non basati sul Web (ad esempio, Active Directory, NTLM, Kerberos)?
Fasi	1. Aggiunta di tutti gli utenti aziendali al provider di identità a. Questi valori possono spesso essere sincronizzati da un sistema HR come Workday, ADP, ecc. 2. Verifica che le informazioni di ciascun utente siano corrette 3. Invio delle informazioni di registrazione ai nuovi utenti per impostare le credenziali di accesso

Applicazione dell'autenticazione a più fattori per tutte le applicazioni

Livello di sforzo	 - **Piccolo sforzo** (se si applica la MFA di base)  - **Sforzo medio** (se si utilizzano chiavi hardware)
Team interessati	• Il team responsabile per il tuo provider di identità (di solito il team di sicurezza o IT) • Gli amministratori che gestiscono le app interne utilizzate da dipendenti e partner
Prodotti	**Provider di identità:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **Proxy inversi dell'applicazione:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Chiavi hardware:** Yubico
Riepilogo	L'autenticazione a più fattori (MFA) è la migliore protezione contro il furto delle credenziali degli utenti tramite phishing o fughe di dati. La maggior parte della MFA può essere abilitata direttamente in un IdP. Per le applicazioni non direttamente integrate con il tuo IdP, prendi in considerazione l'utilizzo di un proxy inverso dell'applicazione davanti all'applicazione per applicare l'autenticazione a più fattori.
Fasi	1. Avviso agli utenti interni dell'imminente imposizione dell'autenticazione a più fattori Specifica delle opzioni per iscriversi agli autenticatori basati su SMS o app 2. Abilitazione di MFA nell'IdP 3. Abilitazione del proxy inverso dell'applicazione davanti alle applicazioni non integrate con il tuo IdP 4. (Bonus) Distribuzione delle chiavi hardware ai dipendenti tramite posta o di persona 5. (Bonus) Applicazione dell'autenticazione a più fattori della chiave hardware per le tue applicazioni più sensibili

Endpoints e dispositivi

Gli endpoint e i dispositivi includono qualsiasi dispositivo, API o servizio software all'interno di un'organizzazione o che ha accesso ai dati dell'organizzazione. Le organizzazioni devono prima comprendere il loro set completo di dispositivi, API e servizi. Quindi le politiche Zero Trust possono essere implementate in base al contesto del dispositivo, dell'API e del servizio.

Implementazione della gestione dei dispositivi mobili

Livello di sforzo	 - **Sforzo medio**
Team interessati	• Team IT
Prodotti	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
Riepilogo	La maggior parte dell'architettura Zero Trust richiede che il software sia installato su almeno un sottogruppo di macchine utente. La gestione dei dispositivi mobili (MDM, Mobile Device Management) è il modo in cui la maggior parte delle organizzazioni gestisce il software e la configurazione nell'inventario dei dispositivi degli utenti.
Fasi	Consulta il sito del fornitore MDM per maggiori dettagli.

Implementazione della protezione degli endpoint

Livello di sforzo	 - **Sforzo medio**
Team interessati	• Team di sicurezza • Team IT
Prodotti	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
Riepilogo	Il software di protezione degli endpoint viene installato sul computer di un utente ed esegue la scansione delle minacce note che colpiscono i dispositivi. Può inoltre essere utilizzato per imporre la conformità delle patch e degli aggiornamenti del sistema operativo. Il segnale del software di protezione degli endpoint può e deve essere utilizzato nelle politiche di controllo degli accessi alle applicazioni.
Fasi	1. Installazione del software di protezione degli endpoint sui computer degli utenti tramite la gestione dei dispositivi mobili 2. Abilitazione della protezione dalle minacce e del controllo della conformità nella piattaforma di protezione degli endpoint

Inventario di dispositivi, API e servizi

Livello di sforzo	- **Piccolo sforzo**
Team interessati	• Team di sicurezza • Team IT
Prodotti	**Inventario dei dispositivi:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **Inventario di API/servizi:** Cloudflare Application Connector, Zscaler Private Access (ZPA)
Riepilogo	Il software di protezione degli endpoint e il software di gestione delle risorse possono essere utilizzati per tenere traccia di tutti i dispositivi che sono stati distribuiti agli utenti. Dovrebbe essere mantenuto un elenco accurato di dispositivi per tenere traccia di quali dispositivi sono validi e dovrebbero avere accesso ad determinate applicazioni. Anche le API e i servizi dovrebbero essere rilevati e conservati in un inventario. La scansione di rete può essere sfruttata per identificare API e servizi software appena visti in grado di comunicare su una rete interna o esterna.
Fasi	1. Installazione del software di protezione degli endpoint sui computer degli utenti tramite la gestione dei dispositivi mobili 2. Installazione dello scanner di API/servizi all'interno della tua rete

Traffico Internet

Il traffico Internet include tutto il traffico degli utenti destinato a siti Web al di fuori del controllo di un'organizzazione. Questo può variare da attività legate all'azienda all'utilizzo personale del sito Web. Tutto il traffico in uscita è soggetto a malware e siti dannosi. Un'organizzazione deve stabilire visibilità e controllo sul traffico degli utenti destinato a Internet.

Blocco delle richieste DNS a minacce note o destinazioni rischiose

Livello di sforzo	 - **Piccolo sforzo**
Team interessati	• Team IT con accesso alla configurazione del router o della macchina • Team di sicurezza
Prodotti	**Filtraggio DNS:** Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
Riepilogo	Il filtraggio DNS può essere applicato tramite la configurazione del router o direttamente su una macchina utente. È uno dei modi più veloci per proteggere gli utenti da siti Web dannosi noti.
Fasi	**Filtraggio DNS:** Aggiorna la configurazione della risoluzione DNS sul Wi-Fi dell'ufficio in modo che punti al servizio di risoluzione DNS appropriato. Questa operazione può essere utilizzata per bloccare siti dannosi noti.

Blocco o isolamento delle minacce dietro SSL/TLS

Livello di sforzo	 - **Sforzo medio**
Team interessati	• Team IT con accesso alla configurazione del router o della macchina • Team di sicurezza
Prodotti	**Decrittografia TLS:** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Isolamento del browser:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

Blocco o isolamento delle minacce dietro SSL/TLS (continua)

Riepilogo	Alcune minacce sono nascoste dietro SSL e non possono essere bloccate solo tramite l'ispezione HTTPS. Per proteggere ulteriormente gli utenti dalle minacce dietro SSL, dovrebbe essere utilizzata la decrittografia TLS.
Fasi	**Decrittografia TLS:** 1. assicurati che il software client corretto sia installato su una macchina utente a. Verifica della presenza di VPN o altri software che potrebbero interferire con il traffico Web in uscita sul dispositivo 2. Configurazione del certificato root sul dispositivo per la decrittografia TLS 3. Abilitazione dei criteri per quando evitare di decrittografare il traffico degli utenti a. Questa operazione dovrebbe essere eseguita per i siti che utilizzano il blocco dei certificati b. Alcune aziende bypassano anche la decrittazione per il traffico personale dell'utente (ad es. banche, social media, ecc.) **Isolamento del browser:** 1. L'isolamento del browser può essere distribuito tramite il software client sul dispositivo o tramite un collegamento di isolamento. Possono essere considerati entrambi gli approcci.

Reti

Per reti si intendono tutte le reti pubbliche, private e virtuali all'interno di un'organizzazione. Le organizzazioni devono prima comprendere il loro insieme esistente di reti e segmentarle per prevenire i movimenti laterali. Quindi, è possibile creare politiche Zero Trust che controllano in modo granulare a quali segmenti di una rete possono accedere utenti, endpoint e dispositivi.

Segmentazione dell'accesso alla rete dell'utente

Livello di sforzo	 **- Grande sforzo**
Team interessati	• Team di sicurezza • Team IT
Prodotti	**Zero Trust Network Access (ZTNA):** Cloudflare Zero Trust (Access e Gateway utilizzati insieme), Netskope Private Access, Zscaler Private Access (ZPA)
Riepilogo	Gli utenti possono generalmente accedere a un'intera rete privata utilizzando una VPN o mentre si trovano nella rete dell'ufficio. Un framework Zero Trust richiede che gli utenti abbiano accesso solo a segmenti specifici della rete necessari per completare una determinata attività. Le soluzioni Zero Trust Network consentono agli utenti di accedere a una rete locale da remoto ma con criteri granulari basati su utente, dispositivo e altri fattori.
Fasi	1. Rendere disponibile la rete privata alla ZTNA a. Di solito un connettore di applicazioni, GRE o tunnel IPSec 2. Installazione del client ZTNA sui dispositivi degli utenti tramite MDM 3. Impostazione dei criteri per segmentare l'accesso degli utenti nella rete privata

Utilizzo di Internet a banda larga per la connettività tra filiali

Livello di sforzo	 **- Grande sforzo**
Team interessati	• Team di network engineering • Team IT
Prodotti	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore

Utilizzo di Internet a banda larga per la connettività tra filiali (continua)

Riepilogo	La connettività tra posizioni di rete private (ad esempio, data center e filiali) è stata sempre stabilita utilizzando linee MPLS (Multi-Protocol Label Switching) o altre forme di collegamenti privati offerti dai fornitori di telecomunicazioni. Questi collegamenti MPLS sono in genere costosi e, poiché Internet di base è diventato di qualità superiore, le organizzazioni possono fornire lo stesso livello di accesso sicuro instradando il traffico su Internet tramite tunnel protetti a una frazione del costo.
Fasi	1. Scegli due posizioni collegate a MPLS con cui iniziare. Queste posizioni avranno bisogno di una qualche forma di connettività Internet. 2. Stabilisci una coppia di tunnel IPsec o GRE Anycast ridondanti sui circuiti Internet verso la rete perimetrale del provider WAN cloud. 3. Verifica l'integrità e la connettività tra quei tunnel. Esegui un test delle prestazioni (throughput, latenza, perdita di pacchetti, jitter) dei carichi di lavoro del traffico il più simile possibile al traffico di produzione. 4. Modifica le politiche di routing per migrare il traffico di produzione da MPLS a tunnel Internet 5. Ripeti le stesse operazioni per la posizione successiva connessa a MPLS 6. Disattivazione dei circuiti MPLS

Chiudere tutte le porte in entrata aperte su Internet per la consegna delle applicazioni

Livello di sforzo	- **Piccolo sforzo**
Team interessati	• Team di network engineering
Prodotti	**Proxy inversi Zero Trust:** Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Riepilogo	Le porte di rete in entrata aperte possono essere trovate utilizzando la tecnologia di scansione e sono un vettore di attacco comune. I proxy inversi Zero Trust consentono di esporre in modo sicuro un'applicazione Web senza aprire porte in entrata. Il record DNS dell'applicazione è l'unico record pubblicamente visibile dell'applicazione. E il record DNS è protetto con le politiche Zero Trust. Come ulteriore livello di sicurezza, il DNS interno/privato può essere sfruttato utilizzando un servizio Zero Trust Network Access (maggiori dettagli di seguito).
Fasi	1. Installazione del connettore dell'applicazione del proxy inverso, in genere un daemon o una macchina virtuale da qualche parte sulla stessa rete 2. Connessione dell'applicazione del proxy inverso al connettore dell'applicazione 3. Chiusura di tutte le porte in entrata sulla rete privata con una regola del firewall

Applicazioni

Con il termine applicazioni si intende qualsiasi risorsa in cui esistono dati organizzativi o vengono eseguiti processi aziendali. Le organizzazioni devono prima comprendere le applicazioni esistenti e quindi stabilire criteri Zero Trust per ciascuna applicazione o, in alcuni casi, bloccare le applicazioni non approvate.

Monitoraggio delle applicazioni di posta elettronica ed esclusione dei tentativi di phishing

Livello di sforzo	- Piccolo sforzo
Team interessati	• Il team responsabile della configurazione del tuo provider di posta elettronica (di solito, IT)
Prodotti	**Sicurezza della posta elettronica su cloud:** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **Isolamento del browser:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
Riepilogo	L'e-mail è uno dei pochi canali di comunicazione tramite il quale gli autori di attacchi hanno libero accesso ai tuoi dipendenti. La distribuzione di un gateway e-mail sicuro è un passaggio fondamentale per garantire che e-mail dannose o non attendibili non raggiungano i dipendenti. Inoltre, i team di sicurezza dovrebbero prendere in considerazione un'opzione per mettere in quarantena i collegamenti in un browser isolato che non sono abbastanza sospetti per essere bloccati completamente.
Fasi	1. Configurazione dei record MX del dominio in modo che puntino al servizio di gateway di posta elettronica sicuro 2. Monitoraggio dei falsi positivi nelle prime settimane 3. (Bonus) Implementazione di un approccio di isolamento del browser basato sui collegamenti per i collegamenti e-mail sospetti al limite.

Inventario di tutte le applicazioni aziendali

Livello di sforzo	- Sforzo medio
Team interessati	• Team di sicurezza
Prodotti	**Secure Web Gateway e CASB con il rilevamento di Shadow IT:** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)

Inventario di tutte le applicazioni aziendali (continua)

Riepilogo	Per un team di sicurezza conoscere l'inventario completo delle applicazioni utilizzate nell'azienda è di fondamentale importanza. Spesso indicate come "Shadow IT", i team di sicurezza scopriranno spesso applicazioni non autorizzate o sconosciute utilizzate nell'azienda. Per identificare le applicazioni, può essere utilizzato un Secure Web Gateway con decrittografia TLS. Il Secure Web Gateway può essere utilizzato anche per bloccare applicazioni o tenant di applicazioni non approvati (ad esempio, account Dropbox personali).
Fasi	1. Abilitazione della scansione Shadow IT nel Secure Web Gateway 2. Verifica che il client Secure Web Gateway sia installato sui dispositivi degli utenti 3. Consentire 2-3 settimane di traffico dagli utenti 4. Esame dell'elenco delle applicazioni identificate 5. Eventuali applicazioni non approvate devono essere bloccate con i criteri del Secure Web Gateway 6. Le applicazioni approvate devono essere protette con criteri Zero Trust

Applicazione dei criteri Zero Trust per le applicazioni

Livello di sforzo	- **Piccolo sforzo** (per la maggior parte delle applicazioni critiche) - **Grande sforzo** (per tutte le applicazioni)
Team interessati	• Team di sicurezza • Team di sviluppo delle applicazioni • Team IT
Prodotti	**Proxy inversi Zero Trust:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Zero Trust Network Access (ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB **Remote Browser Isolation:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

Applicazione dei criteri Zero Trust per le applicazioni (continua)

Riepilogo	Le applicazioni devono essere protette con criteri Zero Trust che considerano l'identità dell'utente, il dispositivo e il contesto di rete prima di autenticarsi e autorizzare l'accesso. Le applicazioni devono avere criteri granulari che impongono il privilegio minimo, in particolare per le applicazioni che contengono dati sensibili. Esistono tre tipi principali di applicazioni e il modello di sicurezza Zero Trust varia per ognuno di essi. I principali tipi di applicazione sono: 1. Applicazioni private self-hosted (indirizzabili solo sulla rete aziendale) 2. Applicazioni pubbliche self-hosted (indirizzabili su Internet) 3. Applicazioni SaaS **Nota:** se il contesto del dispositivo o lo stato di conformità sono criteri di sicurezza obbligatori, in genere è necessario il software client sul dispositivo.
Fasi	**Applicazioni private self-hosted** 1. Crea un tunnel crittografato tra l'applicazione e il livello di criteri Zero Trust. In genere si tratta di un "connettore di applicazioni", GRE o tunnel IPSec. 2. Rendi disponibile il resolver DNS privato per gli utenti del client del dispositivo ZTNA. 3. Crea politiche basate sul contesto di utente, dispositivo e rete per stabilire chi può accedere all'applicazione **Applicazioni pubbliche self-hosted** 1. Sposta il DNS autorevole o un record CNAME nel proxy inverso dell'applicazione 2. Assicurati che tutte le porte in entrata siano chiuse per la rete dell'applicazione 3. Crea politiche basate sul contesto di utente, dispositivo e rete per stabilire chi può accedere all'applicazione **Applicazioni SaaS** Esistono diverse opzioni per applicare i criteri Zero Trust per le applicazioni SaaS. **Proxy di identità** Cloudflare, Netskope e Zscaler forniscono proxy di identità che consentono la stessa applicazione dei criteri di un'applicazione self-hosted del proxy inverso. Ciò richiede che il proxy di identità sia configurato come provider SSO dell'applicazione SaaS. 1. Rimuovi l'integrazione SSO esistente nell'app SaaS, se presente 2. Integra il proxy di identità con l'applicazione SaaS 3. Assicurati che gli attributi SAML corretti vengano inviati per la creazione e gli aggiornamenti degli utenti 4. Crea criteri in base al contesto di utente, dispositivo e rete

Applicazione dei criteri Zero Trust per le applicazioni (continua)

Fasi	**Secure Web Gateway e Single Sign On** L'altro approccio consiste nell'utilizzare un provider Single Sign On esistente per controllare quali utenti possono e non possono accedere all'applicazione SaaS. Quindi il Secure Web Gateway, con un indirizzo IP dedicato, può essere utilizzato per garantire che solo gli utenti dei dispositivi gestiti con ispezione del traffico possano accedere all'applicazione SaaS. 1. Aggiungi l'applicazione SaaS al provider SSO 2. Crea i criteri per imporre quali utenti sono autorizzati 3. Aggiungi l'indirizzo IP dell'istanza di Secure Web Gateway all'elenco di indirizzi IP consentiti dell'applicazione SaaS (la maggior parte delle app SaaS supporta elenchi di indirizzi IP consentiti nelle impostazioni di sicurezza di base) 4. Crea criteri Secure Web Gateway che controllano quali utenti possono accedere all'applicazione SaaS

Proteggi le applicazioni dagli attacchi di livello 7 (DDoS, injection, bot, ecc.)

Livello di sforzo	**- Piccolo sforzo**
Team interessati	• Team di sicurezza • Team di sviluppo delle applicazioni
Prodotti	Akamai, AWS, Azure, Cloudflare, GCP
Riepilogo	Qualsiasi applicazione self-hosted è suscettibile agli attacchi di livello 7, inclusi DDoS, Code Injection, Bot e altro. I team di sicurezza dovrebbero implementare un Web Application Firewall e una protezione DDoS davanti a tutte le applicazioni self-hosted, indirizzabili privatamente e pubblicamente.
Fasi	1. Aggiungi il record DNS autorevole di qualsiasi applicazione pubblica 2. Abilita il Web Application Firewall e la protezione DDoS

Applicazione di HTTPS e DNSsec

Livello di sforzo	- **Piccolo sforzo**
Team interessati	• Team di sicurezza • Team di sviluppo delle applicazioni
Prodotti	Akamai, AWS, Azure, Cloudflare, GCP
Riepilogo	Qualsiasi applicazione Web self-hosted dovrebbe sfruttare HTTPS e DNSSec. Ciò impedisce qualsiasi potenziale sniffing di pacchetti o hijacking del dominio.
Fasi	1. Aggiungi il record DNS autorevole di qualsiasi applicazione pubblica 2. Imposta HTTPS per limitare e abilitare DNSSEC

Prevenzione e registrazione della perdita dei dati

Una volta che hai stabilito tutti gli elementi Zero Trust della tua architettura fino a questo punto, l'architettura genererà grandi volumi di dati su ciò che sta accadendo all'interno della tua rete. A questo punto, è il momento di implementare la prevenzione e la registrazione della perdita di dati. Si tratta di un insieme di processi e strumenti incentrati sul mantenimento dei dati sensibili all'interno di un'azienda e sull'individuazione di eventuali opportunità di fuga di dati. Le organizzazioni devono prima capire dove si trovano i loro dati sensibili. Quindi possono stabilire controlli Zero Trust per bloccare l'accesso e l'esfiltrazione di dati sensibili.

Definizione di un processo per registrare e rivedere il traffico sulle applicazioni sensibili

Livello di sforzo	 - **Sforzo medio**
Team interessati	• Team di sicurezza
Prodotti	**Secure Web Gateway (SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Security Incident and Event Monitoring (SIEM):** DataDog, Splunk, SolarWinds
Riepilogo	Le soluzioni di Secure Web Gateway hanno funzionalità per passare i registri del traffico degli utenti a uno strumento SIEM. Un team di sicurezza dovrebbe eseguire regolarmente la revisione dei registri del traffico destinati alle applicazioni sensibili. Avvisi specifici per traffico anomalo o dannoso possono essere impostati e ottimizzati nel tempo nel SIEM.
Fasi	1. Verifica che tutto il traffico utente destinato alle applicazioni sensibili venga inviato tramite proxy tramite SWG 2. Abilitazione della funzionalità di log push o pull tra il tuo SWG e SIEM 3. Impostazione di un intervallo specifico per il team di sicurezza per la revisione dei registri del traffico 4. Configurazione degli avvisi nel SIEM in base ai risultati nel tempo

Definizione dei dati sensibili e di dove si trovano

Livello di sforzo	 - **Sforzo medio**
Team interessati	• Team di sicurezza • Team di conformità/legale
Prodotti	**Security Incident and Event Monitoring (SIEM):** DataDog, Splunk, SolarWinds

Definizione dei dati sensibili e di dove si trovano (continua)

Riepilogo	I dati sensibili variano ampiamente a seconda del settore. Le aziende tecnologiche sono preoccupate per la protezione del codice sorgente mentre i fornitori di servizi medici sono fortemente concentrati sulla conformità HIPAA. È importante stabilire quali sono i dati sensibili per la tua azienda e dove risiedono. Un'accurata definizione e inventario dei dati sensibili informerà l'implementazione degli strumenti di prevenzione della perdita di dati.
Fasi	1. Esame dei registri del traffico negli strumenti SIEM o direttamente in un Secure Web Gateway per identificare le applicazioni di destinazione e gli archivi dati 2. Fare un inventario dei dati sensibili esistenti

Impedire ai dati sensibili di lasciare le tue applicazioni

Livello di sforzo	- **Grande sforzo**
Team interessati	• Team di sicurezza • Team IT • Team di conformità/legale
Prodotti	**Data Loss Prevention (DLP) in linea:** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
Riepilogo	Le soluzioni DLP in linea ispezionano il traffico degli utenti e gli upload/download di file alla ricerca di dati sensibili. I dati sensibili sono disponibili in elenchi predefiniti noti (ad esempio, PII, SSN, Carte di credito, ecc.) o modelli specifici possono essere configurati manualmente da un amministratore. I controlli DLP devono essere abilitati per le applicazioni sensibili e possono essere espansi per tutto il traffico degli utenti.
Fasi	1. Installazione del software client dal provider DLP 2. Verifica che non esistano VPN o altri strumenti che interrompano la connettività 3. Verifica che la decrittografia TLS sia abilitata e che un certificato root sia presente su ogni macchina utente 4. Abilitazione dei controlli DLP 5. Monitoraggio degli eventi di blocco DLP e verifica se è valido o un falso positivo

Identificazione delle configurazioni errate e i dati condivisi pubblicamente negli strumenti SaaS

Livello di sforzo	- **Piccolo sforzo**
Team interessati	• Team di sicurezza
Prodotti	**Cloud Access Security Broker (CASB) basato su API:** Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
Riepilogo	I CASB si integrano con le principali applicazioni SaaS tramite un'integrazione API. Il CASB eseguirà quindi la scansione dell'applicazione SaaS per individuare errori di configurazione della sicurezza noti e dati che sono stati condivisi pubblicamente. Un team di sicurezza dovrebbe stabilire una cadenza regolare per esaminare i risultati del CASB.
Fasi	1. Connetti ogni applicazione SaaS tramite le istruzioni di integrazione dell'API del provider 2. Esecuzione delle scansioni per ogni applicazione SaaS 3. Esame dei risultati della scansione e inizio della correzione in ciascuna applicazione SaaS, ove appropriato

Definizione un Security Operations Center (SOC) per la revisione dei registri, gli aggiornamenti delle politiche e la mitigazione

Livello di sforzo	- **Sforzo medio**
Team interessati	• Team di sicurezza
Prodotti	**Nessuna**
Riepilogo	Un SOC è una funzione fondamentale all'interno di un team di sicurezza in un framework Zero Trust. Dovrebbe concentrarsi sulla revisione delle informazioni di registro e degli avvisi di sicurezza e sull'adeguamento delle politiche Zero Trust in tutti i prodotti di sicurezza principali.
Fasi	1. Revisione dei log in SIEM o direttamente nel prodotto di sicurezza 2. Identificazione di eventuali avvisi o attività anomale 3. Aggiornamento dei criteri Zero Trust in ogni strumento in base ai risultati

Rimanere aggiornati sui soggetti noti delle minacce

Livello di sforzo	- **Piccolo sforzo**
Team interessati	• Team di sicurezza
Prodotti	**Provider di intelligence delle minacce:** Cloudflare Radar, CISA, OWASP
Riepilogo	Esistono più fornitori focalizzati sulla compilazione di un elenco di soggetti di minacce noti e siti Web dannosi. Questi feed di minacce possono essere caricati automaticamente in un Secure Web Gateway per proteggere gli utenti dagli attacchi.
Fasi	1. Collegamento del feed delle minacce a Secure Web Gateway 2. Abilitazione della protezione dalle minacce nei filtri DNS e HTTP

Stato stazionario

Dopo aver costruito la tua architettura Zero Trust per tutti gli altri elementi della tua organizzazione, ci sono una serie di azioni che puoi intraprendere per portare la tua organizzazione a uno stato stazionario Zero Trust, garantendo la coerenza con l'architettura che va avanti.

Utilizzo di un approccio DevOps per garantire l'applicazione coerente dei criteri per tutte le nuove risorse

Livello di sforzo	**- Grande sforzo**
Team interessati	• Team di sicurezza • Team di sviluppo delle applicazioni
Prodotti	**Automazione dell'infrastruttura:** Ansible, Puppet, Terraform
Riepilogo	Gli strumenti di automazione dell'infrastruttura consentono agli sviluppatori di implementare automaticamente la sicurezza Zero Trust come parte della loro pipeline di sviluppo delle applicazioni. Stabilisci test interni che si attiveranno se un'applicazione viene distribuita con protezione proxy inverso Zero Trust.
Fasi	1. Definizione di una politica standard per le nuove applicazioni 2. Aggiunta di test nel processo di distribuzione dell'applicazione che richiedono la protezione proxy inverso Zero Trust

Implementazione della scalabilità automatica per le risorse on-ramp

Livello di sforzo	**- Grande sforzo**
Team interessati	• Team di sicurezza • Team di sviluppo delle applicazioni
Prodotti	**Bilanciatori di carico:** Akamai, Cloudflare **Automazione dell'infrastruttura:** Ansible, Puppet, Terraform

Implementazione della scalabilità automatica per le risorse on-ramp (continua)

Riepilogo	I bilanciatori di carico possono essere strumenti efficaci per garantire che l'infrastruttura delle singole applicazioni non venga mai sovraccaricata. Oltre a fornire un livello di ridondanza in caso di guasto di un server delle applicazioni. Gli strumenti di automazione dell'infrastruttura possono essere utilizzati per creare nuove risorse se vengono superate soglie di traffico specifiche.
Fasi	1. Configurazione di un bilanciatore di carico davanti al connettore dell'applicazione proxy inverso Zero Trust 2. Abilitazione delle regole di bilanciamento del carico in base ai volumi di traffico e/o alla geolocalizzazione degli utenti 3. Implementazione di criteri di automazione dell'infrastruttura che eseguiranno il provisioning di nuove macchine virtuali se viene generato un carico sufficiente per un set specifico di applicazioni

Sequenza temporale di implementazione di esempio

Ogni implementazione di Zero Trust Architecture è unica, ma ci sono una serie di passaggi comuni seguiti dalla maggior parte dei progetti. Questa è una sequenza temporale consigliata per un'azienda che inizia a implementare un'architettura Zero Trust.

Sequenza temporale		Scopo	Prodotti rilevanti
Fase 1	☐	**Distribuzione del filtraggio DNS globale**	Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
	☐	**Monitoraggio delle e-mail in entrata ed esclusione dei tentativi di phishing**	**Sicurezza della posta elettronica su cloud:** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **Isolamento del browser:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	**Identificazione di una configurazione errata e dei dati condivisi pubblicamente negli strumenti SaaS**	Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
Fase 2	☐	**Definizione dell'identità aziendale**	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
	☐	**Applicazione dell'autenticazione a più fattori di base per tutte le applicazioni**	**Provider di identità:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **Proxy inversi dell'applicazione:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	**Applicazione di HTTPS e DNSsec**	Akamai, AWS, Azure, Cloudflare, GCP
	☐	**Blocco o isolamento delle minacce dietro SSL**	**Decrittografia TLS:** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Isolamento del browser:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	**Applicazione dei criteri ZT per le app indirizzabili pubblicamente**	**Proxy inversi Zero Trust:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	**Protezione delle applicazioni dagli attacchi di livello 7**	Akamai, AWS, Azure, Cloudflare, GCP
	☐	**Chiusura di tutte le porte in entrata aperte su Internet per la consegna delle app**	Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
La Fase 3	☐	**Inventario di tutte le applicazioni aziendali**	**Secure Web Gateway e CASB con il rilevamento di Shadow IT:** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
	☐	**Applicazione dei criteri ZT per le applicazioni SaaS**	**Zero Trust Network Access (ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB

	☐ **Segmentazione dell'accesso alla rete dell'utente**	**Zero Trust Network Access (ZTNA):** Cloudflare Zero Trust (Access e Gateway utilizzati insieme), Netskope Private Access, Zscaler Private Access (ZPA)
	☐ **ZTNA per applicazioni critiche indirizzabili privatamente**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **Implementazione di MDM/UEM per controllare i dispositivi aziendali**	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
	☐ **Definizione dei dati sensibili e di dove si trovano**	DataDog, Splunk, SolarWinds
	☐ **Invio di token di autenticazione basati su hardware**	**Chiavi hardware:** Yubico
	☐ **Rimanere aggiornati sui soggetti noti delle minacce**	Cloudflare Radar, CISA, OWASP
Fase 4	☐ **Applicazione dell'autenticazione a più fattori basata su token hardware**	**Chiavi hardware:** Yubico
	☐ **Applicazione dei criteri ZT e accesso alla rete per tutte le applicazioni**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **Definizione di un SOC per la revisione dei log, gli aggiornamenti dei criteri e la mitigazione**	N/D
	☐ **Implementazione della protezione degli endpoint**	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
	☐ **Inventario di tutti i dispositivi, le API e i servizi aziendali**	**Inventario dei dispositivi:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **Inventario di API/servizi:** Cloudflare Application Connector, Zscaler Private Access (ZPA)
	☐ **Utilizzo di Internet a banda larga per la connettività tra filiali**	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore
	☐ **Definizione di un processo per registrare e rivedere l'attività dei dipendenti sulle applicazioni sensibili**	**Secure Web Gateway (SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Security Incident and Event Monitoring (SIEM):** DataDog, Splunk, SolarWinds
	☐ **Impedire ai dati sensibili di lasciare le tue applicazioni (ad esempio, PII, Carte di credito, SSN, ecc.)**	Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
	☐ **Utilizzo di un approccio DevOps per garantire l'applicazione dei criteri per tutte le nuove risorse**	Ansible, Puppet, Terraform
	☐ **Implementazione della scalabilità automatica per le risorse on-ramp**	**Bilanciatori di carico:** Akamai, Cloudflare **Automazione dell'infrastruttura:** Ansible, Puppet, Terraform

CLOUDFLARE

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

REV:BDES-3584.2022AUG09