WHITE PAPER

La roadmap per un eccellente sistema di sicurezza

Richiedete un piano di trasformazione personalizzato incentrato sul modello Zero Trust

Per garantire alla nostra azienda la massima protezione in un settore in continua evoluzione, come quello della sicurezza (e per evitare di trascurare eventuali rischi), abbiamo recentemente esaminato le performance del nostro sistema di sicurezza tramite la soluzione ZTMM (Zero Trust Maturity Model). Pertanto, desideriamo illustrarvi come fare lo stesso per la vostra organizzazione in modo da evidenziare le aree critiche che richiedono miglioramenti e creare una chiara roadmap utile per un eccellente sistema di sicurezza.

Come semplificare il percorso verso l'adozione del modello Zero Trust

Gli accessi e la sicurezza di un'azienda sono aspetti complessi e in costante evoluzione. In questo contesto, può risultare difficoltoso capire dove è necessario concentrare i propri sforzi nel percorso verso l'adozione di un sistema di sicurezza Zero Trust.

Ecco perché vi consigliamo di utilizzare la soluzione ZTMM per esaminare e valutare il vostro attuale sistema di sicurezza. Noi abbiamo usato questa soluzione per valutare il sistema di sicurezza di Akamai, nonché i sistemi di sicurezza di alcuni dei nostri clienti. Alla fine del processo, avrete a disposizione una roadmap di azioni pratiche in grado di semplificare il vostro percorso verso un'architettura Zero Trust (per ulteriori informazioni sul concetto Zero Trust, potete consultare l'Appendice A).

I vantaggi offerti dalla soluzione ZTMM

Riteniamo che il passaggio più importante nel percorso verso un sistema di sicurezza più solido sia il primo: iniziare. Tuttavia, quando si entra nel complesso settore della cybersecurity in continua evoluzione, iniziare è più facile a dirsi che a farsi. Abbiamo visto che molte organizzazioni hanno difficoltà a decidere cosa fare, quanto fare e come apportare i cambiamenti necessari per adottare il modello Zero Trust.

Ed è a questo punto che entra in gioco la soluzione ZTMM: creando un sistema basato sul modello Zero Trust con un senso di linearità che ne semplifica l'implementazione, aiuta le organizzazioni a pianificare i cambiamenti e ad allocare i budget necessari per gli aggiornamenti; inoltre, spiega i concetti Zero Trust ai responsabili decisionali che non sono esperti IT per aiutare i team IT ad acquisire gli strumenti richiesti.

La collaudata soluzione ZTMM è stata sviluppata dalla CISA (Cybersecurity and Infrastructure Security Agency) ed è ampiamente adottata dalle agenzie federali degli Stati Uniti.

I cinque pilastri e le tre funzionalità fondamentali della soluzione ZTMM

La soluzione ZTMM rappresenta un gradiente di implementazione in cinque pilastri fondamentali per consentire di apportare minime innovazioni nel corso del tempo. I cinque pilastri fondamentali che dovete considerare sono: identità, dispositivi, reti, applicazioni e carichi di lavoro e, infine, dati (Figura 1). La soluzione ZTMM, inoltre, vi richiede di considerare le tre funzionalità che riguardano i cinque pilastri fondamentali:

- Visibilità e analisi
- Automazione e coordinamento
- Governance

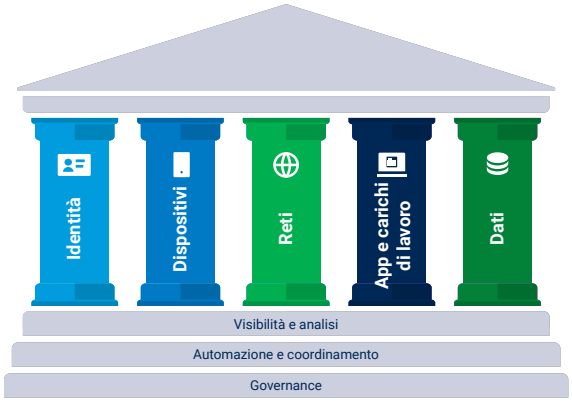


Fig. 1. La soluzione ZTMM della CISA offre uno dei tanti percorsi che supportano il passaggio al modello Zero Trust (fonte: CISA)

Ad ognuna di queste aree viene assegnato un livello di maturità che corrisponde al punto in cui un'organizzazione si trova nel percorso verso l'adozione di un approccio Zero Trust. I quattro livelli di maturità (tradizionale, iniziale, avanzato e ottimale) descrivono il percorso dell'organizzazione partendo dalla configurazione manuale e dalle VPN fino a raggiungere la configurazione ideale di un sistema di "protezione senza perimetro" (Figura 2). Al livello di maturità ottimale, le organizzazioni concedono alle applicazioni privilegi minimi, rifiutano l'autenticazione e l'accesso ai dispositivi vulnerabili, impediscono il diffondersi delle minacce interne e, infine, rilevano e rispondono immediatamente ai problemi di sicurezza (per una descrizione più dettagliata del sistema ZTMM, potete consultare l'Appendice B).

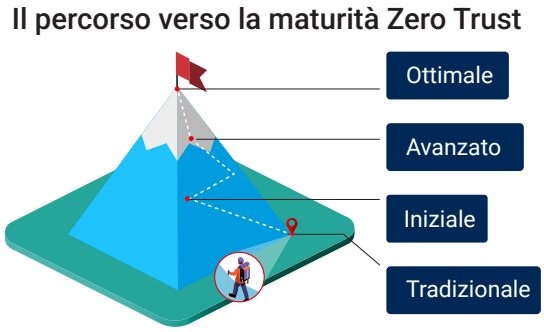


Fig. 2. Il percorso verso la maturità Zero Trust (fonte: CISA)

Mettendo in evidenza le aree che presentano il più basso livello di maturità, la soluzione ZTMM aiuta le organizzazioni a sviluppare un ambiente di sicurezza più bilanciato. L'innovativa gamma di soluzioni per la sicurezza di Akamai, combinata con le nostre competenze, semplifica il passaggio ad un sistema di sicurezza più maturo.

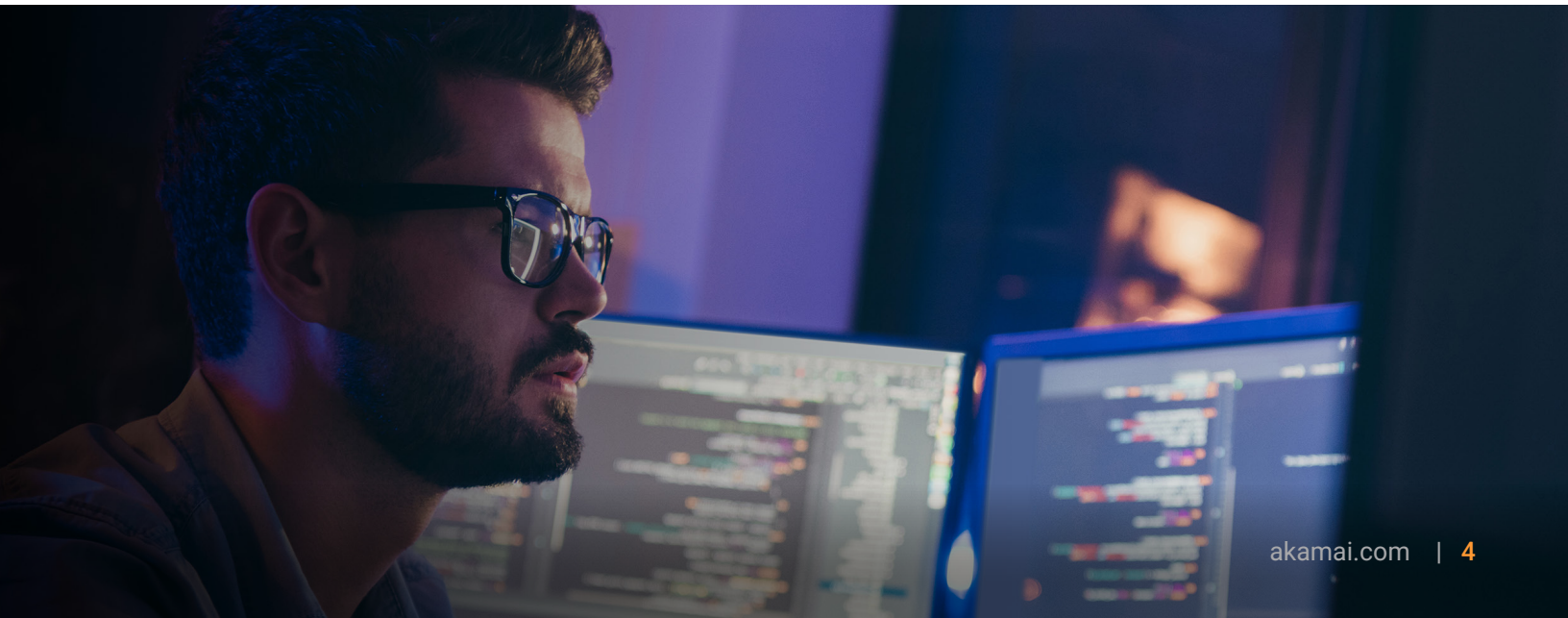
I vostri team hanno problemi ad implementare il modello Zero Trust? Non sono gli unici.

La responsabilità di creare un'architettura Zero Trust non è da imputare ad un solo reparto, ma richiede la capacità di acquisire gli strumenti necessari, di adottare la giusta flessibilità e di approvare le parti coinvolte a tutti i livelli di un'azienda.

Akamai è l'azienda di cybersecurity e cloud computing che abilita e protegge il business online. Le nostre soluzioni di sicurezza leader del settore, l'intelligence sulle minacce di livello superiore e il team addetto alle operazioni globali proteggono applicazioni e dati critici ad ogni punto di contatto, in tutto il mondo. Questa visibilità dettagliata ci consente di capire i problemi più comuni che si riscontrano nel percorso verso l'adozione di un sistema di sicurezza Zero Trust e di aiutare a trovare le giuste soluzioni.

I tre problemi più comuni con l'adozione del modello Zero Trust

1. **Sapere da dove iniziare.** Di solito, consigliamo di iniziare ad acquisire una certa visibilità sui carichi di lavoro e a ridurre la superficie di attacco per rafforzare la resilienza informatica, ma, ovviamente, tutto dipende dal livello di sicurezza attuale dell'azienda.
2. **Conseguire rapidamente i risultati prefissati.** L'adozione di un modello Zero Trust può sembrare un'impresa eroica in cui i team hanno difficoltà a focalizzarsi su ogni singolo aspetto o a rendersi conto dei piccoli progressi compiuti in vista dell'obiettivo prefissato.
3. **Mostrare il ROI.** I progetti Zero Trust sono costosi e, di solito, richiedono cambiamenti culturali, nonché tecnologici, all'interno di un'organizzazione. La capacità di mostrare il ritorno sugli investimenti effettuati (che può concretizzarsi nella riduzione della superficie di attacco, nella mitigazione di una violazione o in un vantaggio economico) è fondamentale, specialmente per i responsabili decisionali e gli addetti alla sicurezza.



Siete pronti ad iniziare il percorso verso l'adozione del modello Zero Trust e ad esaminare il vostro sistema di sicurezza?

Come abbiamo fatto all'interno della nostra azienda, potete usare la soluzione ZTMM per esaminare lo stato di maturità delle misure di sicurezza attualmente adottate dalla vostra azienda. In tal modo, potrete sapere come bilanciare maggiormente il vostro processo e cosa dovete cambiare per implementare un'architettura Zero Trust.

Come Akamai può guidarvi nel percorso verso l'adozione di un sistema di sicurezza Zero Trust

Un'architettura Zero Trust utilizza una serie di controlli e principi diversi per affrontare i vari problemi di sicurezza,

che includono iniziative e roadmap utili per creare un piano di implementazione in grado di soddisfare le esigenze della vostra azienda e conseguire gli obietti prefissati allo scopo di raggiungere un eccellente livello di sicurezza. Questo approccio ci consente di lavorare con voi per creare processi e sistemi di sicurezza efficaci e sostenibili nel lungo termine.

Insieme ad Akamai Cloud, la nostra suite di prodotti per la sicurezza, che include un'innovativa soluzione ZTNA distribuita, funzionalità di microsegmentazione leader del settore, autenticazione multifattore anti-phishing (MFA) e un firewall DNS proattivo, potremo raggiungere un livello ottimale di maturità del vostro sistema Zero Trust. Inoltre, potrete eseguire l'intero sistema con un unico agente e un'unica console (Figura 3).

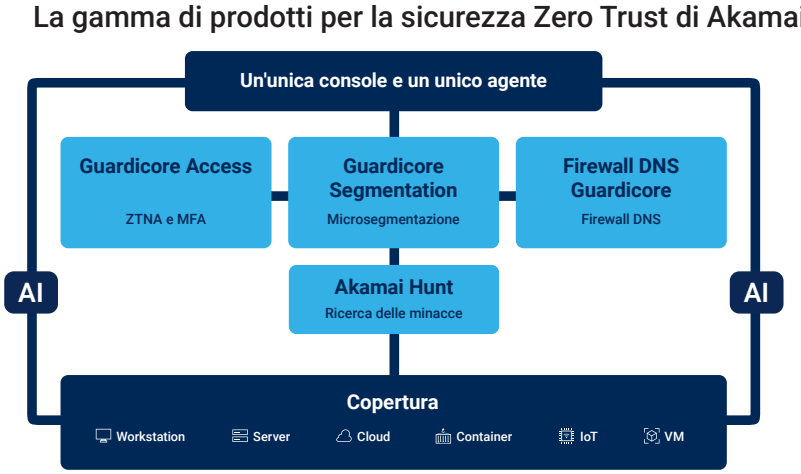


Fig. 3. La gamma di prodotti per la sicurezza di Akamai può essere eseguita con un unico agente e un'unica console

Case study

Valutazione del sistema di sicurezza dell'e-commerce di un retailer multinazionale con la soluzione ZTMM

Recentemente, abbiamo analizzato il sistema di sicurezza dell'e-commerce di un retailer multinazionale, valutando lo stato del suo sistema di sicurezza e fornendo una roadmap corrispondente per migliorare il suo livello di sicurezza. Con la soluzione ZTMM, il nostro team di esperti ha identificato alcune aree da migliorare, che abbiamo classificato in base al loro grado di importanza. Ecco qui di seguito i risultati finali.

Un sistema sbilanciato con implementazioni incoerenti

Per ogni pilastro fondamentale, abbiamo rilevato che alcune funzioni sono state implementate con il massimo livello di maturità (ottimale), come, ad esempio, la gestione dei dispositivi mobili e l'automazione dell'implementazione delle applicazioni. Altre funzioni di ogni pilastro fondamentale, invece, sono rimaste al loro livello tradizionale, presentando, quindi, gravi rischi.

In particolare, non sono state rafforzate alcune importanti funzioni presenti nei pilastri delle identità e delle reti, che costituiscono le fondamenta di un'architettura Zero Trust, tra cui l'MFA, la gestione integrata dell'infrastruttura delle identità, il controllo degli accessi basato sul contesto e la microsegmentazione.

Un'infrastruttura delle identità a rischio

I nostri analisti hanno scoperto che l'autenticazione di ID e password è rimasta al livello standard nel retailer, mentre l'uso dell'MFA è stato limitato a pochi sistemi, il che ha creato un elevato rischio di violazione delle informazioni di autenticazione. Inoltre, è stata rilevata la presenza di più infrastrutture di ID, come, ad esempio, Microsoft Entra ID, AD (Active Directory) on-premise e LDAP (Lightweight Directory Access Protocol). Poiché non è stato integrato il sistema di gestione del retailer, si è riscontrato il rischio di violazioni a partire dall'infrastruttura di ID con misure di sicurezza più deboli, ad esempio LDAP.

Controlli di autorizzazione non integrati

I controlli di autorizzazione non erano stati integrati, quindi ogni applicazione veniva gestita singolarmente. Non era possibile, pertanto, bloccare l'accesso ai dispositivi vulnerabili o ad elementi sospetti: se il PC di un dipendente o di un partner con accesso alla rete dell'azienda veniva infettato da malware, sussisteva un rischio elevato di accessi non autorizzati a sistemi e risorse tramite il movimento laterale.

Una segmentazione inadeguata

Abbiamo scoperto che le misure di sicurezza del retailer erano incentrate notevolmente sulle minacce esterne, trascurando i rischi creati dai criminali che avevano già violato la rete. Senza una solida segmentazione interna, un'intrusione effettuata tramite la rete Wi-Fi in un magazzino o tramite le vulnerabilità presenti in una VPN potrebbe condurre ad un movimento laterale non controllato. Questa mancanza di barriere interne ha aumentato notevolmente il rischio di una diffusa violazione dei sistemi, di fughe di dati e di interruzioni operative in quanto l'attacco potrebbe muoversi liberamente nella rete se non sono state messe in atto delle misure di contenimento.

Una scarsa gestione delle vulnerabilità e delle risposte

Il retailer non disponeva di un sistema di gestione per collegare una distinta "base" dei software (SBOM) con le informazioni sulle vulnerabilità, quindi non poteva identificare e rispondere rapidamente alle vulnerabilità delle applicazioni, che rappresentavano un serio rischio.

I nostri consigli

Per rafforzare il proprio sistema di sicurezza, abbiamo consigliato ai retailer di effettuare le cinque operazioni riportate di seguito:

1. Adottare misure proattive per ridurre i rischi di intrusioni non autorizzate e di movimento laterale consentiti dalla configurazione attuale
2. Continuare ad integrare l'infrastruttura delle identità negli strumenti tecnologici esistenti
3. Sviluppare un piano di espansione delle funzionalità di autenticazione e autorizzazione insieme all'utilizzo della soluzione ZTNA (Zero Trust Network Access)
4. Stabilire il modo più efficace per implementare un sistema granulare per la protezione di applicazioni e carichi di lavoro
5. Creare un sistema e un processo di risposta per le future minacce sconosciute, sviluppare un sistema e un processo per rafforzare la gestione delle vulnerabilità e delle risposte e formulare un piano adeguato

Se siete interessati ad intraprendere il percorso verso il modello Zero Trust, contattateci per pianificare una valutazione gratuita del vostro sistema di sicurezza.

Appendice A. Una panoramica sul concetto Zero Trust

Il modello Zero Trust si basa su una filosofia della sicurezza incentrata sull'idea secondo cui nessun utente, dispositivo o sistema, sia esso interno o esterno alla rete aziendale, deve essere considerato attendibile,

ma che, invece, è necessario usare appositi processi di verifica e monitoraggio per minimizzare i rischi, tra cui applicare rigorose policy per la gestione delle identità e degli accessi (IAM), utilizzare l'autenticazione multifattore (MFA) e dare priorità al controllo degli accessi basato sui ruoli (RBAC).

Il concetto Zero Trust è in circolazione da 15 anni, ma ha assunto una maggiore importanza durante la pandemia di COVID-19 quando le aziende si sono trovate ad affrontare una maggiore richiesta di accessi remoti. Molte aziende hanno capito che le loro misure di sicurezza non riuscivano a stare al passo con la nuova domanda se utenti e dispositivi erano dislocati in varie posizioni anziché centralizzati.

Oggi, esistono molte implementazioni dei principi Zero Trust, come l'architettura Zero Trust, le soluzioni ZTNA (Zero Trust Network Access) e SWG (Secure Web Gateway) con Zero Trust e la microsegmentazione.

Ulteriori informazioni sul modello Zero Trust

Appendice B. Il sistema ZTMM 2.0

I cinque pilastri fondamentali

Ogni pilastro può progredire al proprio ritmo, anche più rapidamente rispetto agli altri, finché non è richiesta una coordinazione tra un pilastro e l'altro.

Pilastro	Descrizione
Identità	Uno o più attributi che descrivono in modo univoco un utente o un'entità, anche diverse dalle persone
Dispositivi	Una risorsa che può connettersi ad una rete, inclusi server, computer desktop e laptop, stampanti, telefoni cellulari, dispositivi IoT (Internet of Things), apparecchiature di rete e molto altro
Reti	Un mezzo di comunicazione aperto, inclusi i canali standard, come reti interne di agenzie, reti wireless e Internet, nonché altri potenziali canali utilizzati per la trasmissione di messaggi
Applicazioni e carichi di lavoro	Sistemi di agenzie, programmi informatici e servizi eseguiti on-premise, sui dispositivi mobili e in ambienti cloud
Dati	File e frammenti strutturati e non strutturati che si trovano o si trovavano in sistemi, dispositivi, reti, applicazioni, database, infrastrutture e backup, nonché i metadati associati

Funzionalità tra pilastri

Le tre funzionalità riportate di seguito supportano l'intero sistema Zero Trust, garantendo l'integrazione, la tempestività e la coerenza delle misure di sicurezza.

Funzionalità	Descrizione
Visibilità e analisi	Le organizzazioni devono disporre di una visibilità chiara e in tempo reale su tutte le attività degli utenti, sullo stato dei dispositivi e sulle interazioni di rete. Le minacce vengono rilevate e mitigate rapidamente per ridurre i rischi. Le organizzazioni prendono decisioni sulla sicurezza informate e proattive.
Automazione e coordinamento	L'errore umano è una causa comune dei problemi di sicurezza. Se le operazioni di automazione e coordinamento vengono ottimizzate, si riducono le possibilità che si verifichi un errore umano. L'automazione semplifica le attività di routine e il coordinamento organizza le operazioni di sicurezza tra i vari sistemi per creare le giuste condizioni allo scopo di velocizzare e coordinare meglio le risposte alle minacce.
Governance	Una buona governance della sicurezza crea un senso di fiducia, assicurando a tutti di seguire le stesse pratiche e le normative sulla sicurezza per creare una solida base allo scopo di proteggere le operazioni. Inoltre, stabilisce chiare linee guida ispirate ai principi Zero Trust e aiuta le organizzazioni a soddisfare gli standard di conformità.

Il livello di maturità della soluzione ZTMM

La soluzione ZTMM 2.0 definisce quattro livelli di maturità per ciascuna funzione. L'obiettivo è stabilire l'attuale livello di maturità dei cinque pilastri e delle tre funzionalità fondamentali, quindi creare un piano per portare ciascuno di questi elementi verso il livello di maturità più elevato.

Livello di maturità	Descrizione
Tradizionale	Configurazione manuale, risposta e mitigazione; policy e soluzioni statiche e compartimentizzate
Iniziale	Avvio dell'automazione; soluzioni iniziali tra un pilastro e l'altro; alcuni cambiamenti reattivi del privilegio minimo; visibilità aggregata per i sistemi interni
Avanzato	Controlli automatizzati, ove applicabili; applicazione delle policy tra un pilastro e l'altro; cambiamenti del privilegio minimo basati sui rischi/livelli; risposta alle mitigazioni predefinite
Ottimale	Controlli automatizzati, ove applicabili; applicazione delle policy tra un pilastro e l'altro; cambiamenti del privilegio minimo basati sui rischi/livelli; risposta alle mitigazioni predefinite

Contattateci per informazioni sulla suite di soluzioni per la sicurezza di Akamai e su come possiamo fare la differenza nel lungo termine per la sicurezza della vostra organizzazione.