Akamai

WHITE PAPER

Raggiungere la maturità Zero Trust con Akamai

A supporto delle capacità intersettoriali di CISA per gli enti e le agenzie federali

Introduzione

La sicurezza Zero Trust è diventata lo standard di riferimento per la protezione dei dati sensibili del governo, delle infrastrutture critiche e dei sistemi di sicurezza nazionale. Gli enti e le agenzie federali non possono continuare ad affidarsi ai modelli tradizionali di sicurezza perimetrali per contrastare le minacce moderne. Di fronte a criminali informatici che diventano sempre più sofisticati e utilizzano tattiche avanzate quali furto di credenziali, ransomware e attacchi dall'interno, gli enti federali stanno spostando sempre più il livello di sicurezza verso un sistema di tipo Zero Trust. Tuttavia, questo cambiamento è stato finora frammentato ed è necessario fare di più per proteggere i sistemi federali.

Il modello di maturità Zero Trust di CISA (Cybersecurity and Infrastructure Security Agency) può aiutare gli enti e le agenzie federali a implementare principi di sicurezza che eliminano la fiducia implicita e applicano rigorosi meccanismi di verifica. Il modello si basa su cinque pilastri fondamentali: identità, dispositivi, reti, applicazioni e carichi di lavoro e, infine, dati. Inoltre, tre funzionalità trasversali, vale a dire visibilità e analisi, automazione e coordinamento e governance, assicurano un approccio olistico e coerente alla cybersicurezza.

Per raggiungere questi obiettivi, la microsegmentazione deve essere considerata un principio fondamentale della sicurezza Zero Trust, che opera come componente fondamentale della difesa della rete interna, vale a dire in direzione est-ovest. Segmentando i carichi di lavoro e limitando il movimento laterale, gli enti federali possono contenere potenziali violazioni e applicare policy di tipo Zero Trust. Inoltre, l'implementazione di soluzioni complete per la sicurezza delle API (Application Programming Interface) consentirà di proteggere le comunicazioni esterne (comunicazioni nord-sud), garantendo che solo le entità autorizzate siano in grado di accedere alle applicazioni governative.

In questo white paper vengono illustrati i passaggi essenziali per raggiungere la maturità Zero Trust, evidenziando il modo in cui le soluzioni avanzate per la sicurezza di Akamai, comprese Akamai Guardicore Segmentation, Akamai API Security e Akamai Enterprise Application Access, consentono agli enti e alle agenzie federali di rispettare le linee guida CISA e migliorare il proprio livello di cybersicurezza.

Il passaggio dalla sicurezza perimetrale alla sicurezza Zero Trust

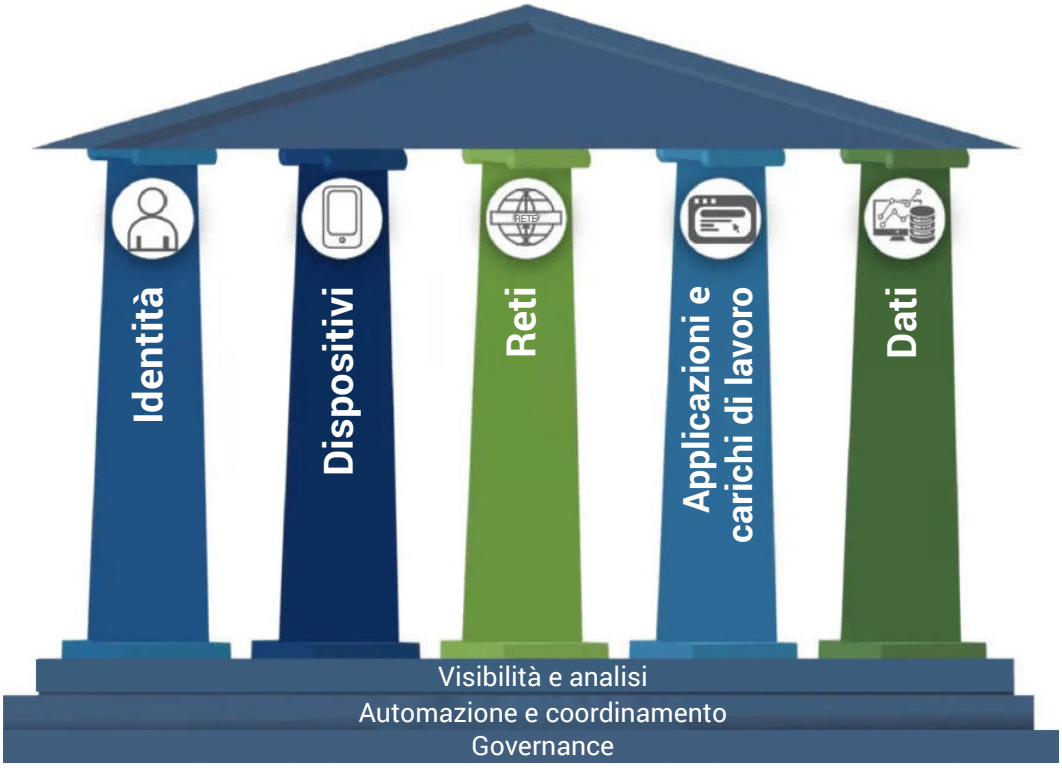
La cybersicurezza tradizionale si basava su difese perimetrali, presupponendo l'affidabilità delle entità già all'interno della rete. Tuttavia, questo modello ha ripetutamente fallito di fronte alle moderne minacce informatiche. I criminali informatici sfruttano credenziali deboli e impostazioni di sicurezza mal configurate e utilizzano tecniche di movimento laterale per bypassare le difese tradizionali e ottenere l'accesso a informazioni sensibili.

L'approccio Zero Trust elimina la fiducia implicita richiedendo la verifica continua di utenti, dispositivi, applicazioni e traffico di rete. Ogni richiesta di accesso viene autenticata, autorizzata e monitorata in modo costante in base a valutazioni dei rischi in tempo reale. Questo approccio riduce drasticamente la superficie di attacco e impedisce l'accesso non autorizzato, anche in caso di violazioni di parte della rete.

Modello di maturità Zero Trust di CISA

Il modello di maturità Zero Trust di CISA fornisce agli enti e alle agenzie federali una roadmap per rafforzare progressivamente il proprio sistema di sicurezza (Figura). Il modello si basa su cinque pilastri fondamentali:

- **Identità:** applicazione di efficaci controlli di autenticazione, autorizzazione e accesso per garantire che solo gli utenti legittimi possano interagire con le risorse sensibili
- **Dispositivi:** monitoraggio, protezione e convalida dei dispositivi endpoint per garantirne la conformità alle policy di sicurezza prima dell'accesso alle reti governative
- **Reti:** implementazione di una microsegmentazione e di policy avanzate di controllo degli accessi per prevenire movimenti laterali non autorizzati
- **Applicazioni e carichi di lavoro:** protezione di applicazioni e carichi di lavoro con rigorose policy di accesso basato sulle identità, sicurezza di runtime e controlli di sicurezza delle API
- **Dati:** impegno perché i dati governativi sensibili rimangano crittografati, monitorati e protetti da accesso ed esfiltrazione non autorizzati



Pilastri del modello di maturità Zero Trust di CISA (Fonte: CISA)

Oltre a questi pilastri, il modello integra tre funzionalità critiche trasversali che si applicano a tutti i componenti dell'approccio Zero Trust:

- **Visibilità e analisi:** monitoraggio continuo, registrazione e rilevamento delle anomalie per identificare e mitigare le minacce in tempo reale
- **Automazione e coordinamento:** automazione della sicurezza basata sull'intelligenza artificiale per applicare policy, rispondere alle minacce e semplificare il controllo degli accessi
- **Governance:** applicazione centralizzata delle policy per garantire la conformità ai mandati federali, come il FISMA (Federal Information Security Modernization Act) e il NIST (National Institute of Standards and Technology), pubblicazione speciale 800-207

L'importanza della microsegmentazione e della sicurezza delle API

Nei modelli tradizionali di sicurezza delle reti, le reti sono in genere suddivise in ampi segmenti utilizzando dei firewall. Sebbene questo approccio offra un certo livello di sicurezza, non garantisce la granularità necessaria per proteggere in modo completo gli ambienti moderni e distribuiti. Negli ambienti federali, la segmentazione basata sulla rete ha in genere come risultato un provisioning eccessivo, vale a dire che utenti e applicazioni hanno accesso a più risorse di quanto sia loro realmente necessario. Questo crea opportunità indesiderate di movimento laterale. Quando gli autori degli attacchi compromettono una parte della rete, sono in grado di spostarsi in aree più sensibili incontrando poca resistenza.

Il concetto di microsegmentazione affronta questo problema introducendo un controllo granulare sul traffico orizzontale (est-ovest) all'interno della rete. In un ambiente microsegmentato, ogni applicazione, carico di lavoro o servizio è isolato dagli altri e l'accesso è limitato in base a policy specifiche. Questo garantisce che utenti, dispositivi e applicazioni possano comunicare solo con le risorse a cui sono esplicitamente autorizzati ad accedere. Implementando una segmentazione basata sulle identità e sulle applicazioni, la microsegmentazione limita i potenziali danni causati dagli attacchi informatici, riduce la superficie di attacco e applica il principio di Zero Trust.

Quando si tratta di traffico di rete verticale (nord-sud), le reti federali si affidano sempre più alle API per facilitare la comunicazione tra i sistemi. Di conseguenza, la protezione degli endpoint delle API diventa una priorità assoluta. Negli ultimi anni gli attacchi alle API, tra cui injection attacks, credential stuffing e accesso non autorizzato ai dati, sono aumentati drasticamente. Gli enti e le agenzie federali hanno bisogno di soluzioni complete per la sicurezza delle API che offrano una protezione dell'intero ciclo di vita delle API, consentendo al personale addetto alla sicurezza di rilevare, monitorare e proteggere il traffico delle API in tempo reale. L'individuazione delle API è particolarmente importante, poiché non è raro che esistano API di cui nessuno è a conoscenza.

Panoramica delle soluzioni Zero Trust di Akamai

Identità

Akamai MFA è una soluzione per la gestione delle identità FIDO2 senza chiave che protegge gli account dei dipendenti dal phishing e da altri attacchi di tipo MITM (Machine-In-The-Middle). Garantisce che solo i dipendenti con un'efficace autenticazione basata sull'identità possano accedere ai propri account. Viene negato qualsiasi altro accesso e viene impedito il controllo degli account dei dipendenti.

Dispositivi

Akamai Guardicore Segmentation è una soluzione di microsegmentazione leader del settore, concepita per limitare la diffusione est-ovest del ransomware e di altri malware. Monitorando e applicando in modo costante le policy sui dispositivi, Akamai Guardicore Segmentation può verificare le configurazioni dei dispositivi, le installazioni del software e le potenziali vulnerabilità, garantendo che solo i dispositivi conformi possano accedere alla rete. Inoltre, la soluzione supporta un approccio senza agenti per proteggere i dispositivi IoT (Internet of Things).

Akamai Enterprise Application Access è una soluzione Zero Trust Network Access completa che garantisce che solo gli utenti e i dispositivi autenticati possano accedere alle applicazioni. Verificando l'identità e il livello dei dispositivi, Enterprise Application Access integra le funzionalità di Akamai Guardicore Segmentation. Se un dispositivo risulta non conforme o presenta un rischio per la sicurezza, Enterprise Application Access può limitarne l'accesso alle applicazioni sensibili.

Reti

Akamai API Security offre ai professionisti della sicurezza federale visibilità completa sull'intero patrimonio di API attraverso l'individuazione continua e l'analisi in tempo reale del traffico nord-sud. La soluzione rileva le API sconosciute, identifica le vulnerabilità e analizza il comportamento delle API in modo che i team addetti alla sicurezza possano rilevare gli attacchi e mitigare i rischi in questa superficie di attacco in rapida espansione.

Akamai App & API Protector riunisce la protezione di Web Application Firewall, mitigazione dei bot, API Security e la protezione da attacchi DDoS (Distributed Denial-of-Service) di livello 7 in un'unica soluzione. Identifica rapidamente le vulnerabilità e mitiga le minacce sull'intera rete e sulle API dell'azienda.

Akamai Secure Internet Access Enterprise è un DNS (Domain Name Service) sicuro basato sul cloud che permette a utenti e dispositivi una connessione sicura a Internet ovunque si trovino, senza la complessità e i costi di gestione associati alle altre soluzioni per la sicurezza.

Akamai Guardicore Segmentation offre un controllo granulare sul traffico di rete, garantendo che sia consentito solo il traffico legittimo.

Panoramica delle soluzioni Zero Trust di Akamai

Applicazioni e carichi di lavoro

Akamai Enterprise Application Access fornisce l'accesso Zero Trust a dipendenti, collaboratori di terze parti, partner e utenti mobili, indipendentemente dalla loro posizione.

Akamai Guardicore Segmentation offre visibilità e comprensione delle applicazioni e dei carichi di lavoro.

Dati

Akamai Secure Internet Access Enterprise offre un accesso sicuro ai dati con funzionalità quali filtraggio dei contenuti, protezione avanzata dalle minacce e prevenzione della perdita di dati. Supporta la gestione dell'inventario dei dati impedendo accessi non autorizzati e perdite di dati.

Akamai Guardicore Segmentation: la chiave per la protezione est-ovest

Akamai Guardicore Segmentation è una soluzione di microsegmentazione leader del settore progettata per aiutare le organizzazioni, in particolare gli enti e le agenzie federali, a implementare controlli di sicurezza granulari in ambienti on-premise e nel cloud

Segmentazione granulare di carichi di lavoro e applicazioni

A differenza della segmentazione tradizionale, che controlla l'accesso a livello di rete, Akamai Guardicore Segmentation applica policy di sicurezza a livello di applicazione e carico di lavoro, garantendo così che l'accesso sia rigorosamente limitato. Ad esempio, in un'agenzia federale, un'applicazione per le risorse umane (HR) può essere limitata alla comunicazione con il solo database delle risorse umane designato, impedendo agli autori degli attacchi di muoversi lateralmente in caso di violazione.

Microsegmentazione basata sull'identità

Akamai Guardicore Segmentation applica la segmentazione in base all'identità degli utenti e dei dispositivi anziché solo agli indirizzi IP. Questo garantisce che l'accesso venga concesso dinamicamente in base al ruolo, al livello di affidabilità e alla verifica in tempo reale. Ad esempio, collaboratori e partner di terze parti possono essere limitati solo ai sistemi di cui hanno bisogno, riducendo i rischi di accesso non autorizzato.

Applicazione dinamica delle policy

Akamai Guardicore Segmentation regola continuamente le policy di sicurezza in base a una serie di fattori in tempo reale, quali il comportamento degli utenti, lo stato dei dispositivi e l'attività della rete. Se viene rilevata un'attività sospetta, ad esempio un volume anomalo di trasferimenti di dati, Akamai Guardicore Segmentation può limitare automaticamente l'accesso, bloccare il traffico o avvisare i team addetti alla sicurezza. Questo approccio proattivo assicura l'evoluzione delle policy di sicurezza per contrastare le minacce emergenti.

Integrando la microsegmentazione di Akamai Guardicore Segmentation, le organizzazioni possono rafforzare la propria architettura Zero Trust, ridurre al minimo i rischi e mantenere un rigoroso controllo degli accessi sulle proprie reti.

CASE STUDY

Akamai Guardicore Segmentation in un ambiente federale

Un'agenzia federale ha recentemente implementato la soluzione di microsegmentazione di Akamai per proteggere i propri sistemi interni dagli attacchi basati sul movimento laterale. Prima di adottare Akamai Guardicore Segmentation, l'agenzia si affidava alla tradizionale segmentazione basata sulla rete, che forniva una granularità limitata e consentiva un ampio accesso tra i diversi segmenti della rete. Questo creava rischi significativi di movimento laterale in caso di compromissione di una parte della rete.

Con Akamai Guardicore Segmentation, l'agenzia è stata in grado di:

- Implementare la segmentazione granulare: segmentando i carichi di lavoro a livello di applicazione, l'agenzia ha ridotto il rischio di movimento laterale e ha garantito che ogni applicazione potesse comunicare solo con le risorse necessarie.
- Migliorare la visibilità: gli strumenti di visualizzazione della soluzione hanno fornito all'agenzia informazioni approfondite sul traffico interno, consentendo ai team addetti alla sicurezza di identificare e mitigare potenziali minacce in tempo reale.
- Migliorare la sicurezza: integrando Akamai Guardicore Segmentation con i sistemi di gestione delle identità e controllo degli accessi esistenti, l'agenzia è stata in grado di applicare l'approccio Zero Trust nell'intera rete, garantendo che l'accesso fosse continuamente monitorato e regolato dinamicamente in base a valutazioni dei rischi in tempo reale.

Questo esempio dimostra la potenza di Akamai Guardicore Segmentation per migliorare la sicurezza della rete, ridurre il rischio di movimento laterale e garantire che le autorizzazioni siano sempre mantenute al minimo necessario.

Sicurezza delle API: protezione del traffico nord-sud

Akamai offre diverse soluzioni per garantire la sicurezza delle API. La piattaforma API Security di Akamai assicura visibilità completa sulle interazioni delle API e rileva e mitiga automaticamente le minacce nord-sud in tempo reale. Grazie all'analisi comportamentale avanzata, gli enti e le agenzie federali sono in grado di:

- **Identificare le API ombra** che potrebbero essere sfruttate da criminali informatici
- **Monitorare i modelli di traffico delle API** per rilevare i tentativi di accesso non autorizzati
- **Implementare la limitazione di velocità delle API** per prevenire abusi e attacchi Denial-of-Service
- **Identificare le API dimenticate, trascurate o sconosciute** per scoprire potenziali percorsi di attacco
- **Inventariare tutte le API,** indipendentemente dalla configurazione o dal tipo, inclusi RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC

Akamai Secure Internet Access Enterprise è un firewall DNS basato sul cloud progettato per aiutare i team addetti alla sicurezza a garantire a tutti gli utenti e dispositivi, all'interno e all'esterno della rete, una connessione sicura a Internet. Questa soluzione blocca in modo proattivo le richieste DNS dannose, tra cui malware, ransomware, phishing ed esfiltrazione di dati DNS a bassa velocità. Secure Internet Access Enterprise riduce la complessità della sicurezza grazie alla assenza di appliance da distribuire, gestire e aggiornare. La soluzione è semplice e intuitiva da usare.

Akamai App & API Protector riesce a individuare e mitigare le minacce basate sulle API per app e API eseguite su Akamai Connected Cloud ed è in grado di bloccare il traffico contenente potenziali minacce non rilevate da Akamai API Security. Se utilizzati insieme, i sistemi di protezione delle API di Akamai offrono un livello completo e costante di visibilità sulle API, consentendo al personale addetto alla sicurezza di individuare, controllare, rilevare e rispondere a eventuali problemi di sicurezza delle API nell'intero patrimonio delle applicazioni.

Funzionalità trasversali con Zero Trust

Una delle principali sfide delle architetture Zero Trust è il rischio di creare dei silos di tecnologia. Spesso ogni area isolata opera in modo indipendente, determinando controlli di sicurezza, misure di policy e rilevamento delle minacce frammentati. Pertanto, l'integrazione tra tutti i livelli di sicurezza è di fondamentale importanza.

Per gli enti e le agenzie federali che gestiscono dati altamente sensibili e infrastrutture complesse, questo approccio frammentato può introdurre rischi significativi per la sicurezza. I criminali informatici possono sfruttare la mancanza di visibilità tra i silos o i pilastri o sfruttare una applicazione delle policy non coerente su sistemi diversi. Per mitigare questi rischi, gli enti federali devono adottare un modello di sicurezza unificato e trasversale che integra visibilità, governance e automazione in tutti i pilastri, garantendo un'applicazione coerente delle policy e riducendo le eventuali lacune che gli avversari possono sfruttare.

Per ottenere un modello di sicurezza unificato, l'integrazione trasversale sui pilastri deve concentrarsi sulle tre aree trasversali del modello di maturità Zero Trust di CISA: visibilità e analisi, automazione e coordinamento e governance. Questi elementi sono essenziali per consentire un'architettura Zero Trust, in cui accesso e autorizzazioni vengono adattati dinamicamente in tutti i pilastri in base a valutazioni dei rischi in tempo reale.

Visibilità e analisi

La visibilità è fondamentale per rilevare le minacce, comprendere il comportamento degli utenti e applicare policy di sicurezza dinamiche a tutti i pilastri. Senza piena visibilità sull'interazione di identità, dispositivi, applicazioni e dati, i team addetti alla sicurezza brancolano nel buio, perché diventa difficile rilevare comportamenti anomali o tentativi di accesso non autorizzati. Le soluzioni di Akamai offrono una visibilità completa e trasversale su tutti i pilastri.

- Akamai Guardicore Segmentation monitora il traffico di rete tra i carichi di lavoro segmentati, fornendo visibilità sul traffico est-ovest e rilevando eventuali tentativi di movimento laterale all'interno della rete.
- Enterprise Application Access fornisce informazioni approfondite sui modelli di accesso alle applicazioni, monitorando il modo in cui gli utenti interagiscono con le applicazioni sensibili e assicurando che l'accesso venga regolato dinamicamente in base ai dati contestuali.

Integrando queste funzionalità, gli enti federali possono mettere in correlazione i dati su tutti i pilastri, consentendo una visione unificata degli eventi di sicurezza. Quando un utente richiede l'accesso a un'applicazione, le soluzioni di Akamai possono controllare non solo l'identità dell'utente, ma anche la sicurezza del dispositivo, la rete utilizzata e il comportamento in tempo reale dell'applicazione. Questo consente ai team addetti alla sicurezza di rilevare più rapidamente potenziali minacce, ridurre al minimo il rischio di escalation dei privilegi e garantire che le autorizzazioni vengano modificate dinamicamente in risposta alle valutazioni dei rischi in tempo reale.

Automazione e coordinamento

Rispondere agli incidenti e applicare policy su più sistemi può essere un processo lento e manuale. Con l'approccio Zero Trust, le policy di sicurezza devono essere applicate dinamicamente a tutti i pilastri, il che richiede un elevato livello di automazione e coordinamento. In questo modo, con il variare dei livelli di rischio, le autorizzazioni vengono immediatamente regolate al livello minimo necessario, riducendo le possibilità di errore umano o di risposta ritardata. Le soluzioni di Akamai offrono flussi di lavoro automatizzati che abbracciano la sicurezza dell'identità, della rete e delle applicazioni.

- Akamai Guardicore Segmentation offre una microsegmentazione automatica, che regola dinamicamente le policy di segmentazione della rete in base ai modelli di traffico e alle anomalie rilevate in tempo reale. Questo garantisce che qualsiasi attività sospetta all'interno della rete venga rapidamente isolata, impedendo il movimento laterale.
- Enterprise Application Access automatizza il processo di protezione dell'accesso alle applicazioni, garantendo che gli utenti possano accedere alle applicazioni solo tramite un proxy sicuro e che le autorizzazioni vengano continuamente aggiornate in base ai fattori di rischio in costante evoluzione.

Automatizzando questi processi, gli enti e le agenzie federali possono garantire che le policy di sicurezza vengano applicate in modo coerente e rapido, riducendo la finestra di opportunità per i criminali informatici.

Governance

La governance è il fondamento di qualsiasi strategia di sicurezza, perché garantisce che le policy siano applicate in modo coerente e che i requisiti di conformità siano soddisfatti. In un modello trasversale o basato su più pilastri, la governance deve garantire che tutti i controlli di sicurezza siano allineati ai principi di Zero Trust. Con le soluzioni di Akamai, le agenzie possono implementare policy di governance che abbracciano tutti i pilastri.

- Governance delle identità: garantire che i controlli degli accessi basati sulle identità vengano applicati in modo coerente su dispositivi, applicazioni e reti e che le autorizzazioni di accesso vengano riviste e aggiornate periodicamente in base a valutazioni dei rischi in tempo reale
- Governance della rete: applicare policy di segmentazione della rete e monitoraggio del traffico in tutti gli ambienti, incluse le infrastrutture locali, cloud e ibride; Akamai Guardicore Segmentation consente alle agenzie di definire policy di segmentazione della rete e di garantire che vengano applicate in modo coerente nell'intera infrastruttura
- Governance dei dati: proteggere i dati sensibili garantendo che l'accesso sia limitato in base al privilegio minimo e che tutti i trasferimenti di dati siano costantemente monitorati per l'accesso non autorizzato o attività sospette

Le tecnologie di Akamai sono progettate per lavorare insieme in modo ottimale per fornire agli enti federali un'architettura di sicurezza basata trasversalmente su più pilastri e completamente integrata che supporta l'approccio Zero Trust.

CASE STUDY

Integrazione trasversale a più pilastri in un'agenzia federale

Una grande agenzia federale ha dovuto affrontare sfide significative legate a policy di sicurezza frammentate a livello di identità, rete e applicazione. Sistemi diversi gestivano la verifica delle identità, l'accesso alle applicazioni e la segmentazione della rete, determinando un'applicazione non coerente delle policy di sicurezza e lacune di visibilità.

Adottando le soluzioni integrate di Akamai, l'agenzia è stata in grado di:

- **Unificare la sicurezza delle identità e delle applicazioni:** è stata integrata Enterprise Application Access, la soluzione di gestione delle identità, delle credenziali e degli accessi (ICAM, Identity, Credential and Access Management) di Akamai, per garantire che l'accesso alle applicazioni fosse sempre autenticato in base ai dati delle identità in tempo reale. Questo ha consentito all'agenzia di regolare dinamicamente le autorizzazioni dell'applicazione in base al comportamento degli utenti e allo stato dei dispositivi.
- **Applicare la segmentazione dinamica della rete:** è stata implementata Akamai Guardicore Segmentation per segmentare il traffico di rete in base alle identità e all'accesso alle applicazioni, impedendo il movimento laterale tra i sistemi sensibili e garantendo che le autorizzazioni fossero costantemente aggiornate in base a valutazioni dei rischi in tempo reale.
- **Migliorare la visibilità e l'automazione:** l'agenzia ha utilizzato gli strumenti integrati di analisi e automazione di Akamai per ottenere una visibilità completa sul proprio livello di sicurezza e per automatizzare l'applicazione delle policy in tutti i pilastri.

Di conseguenza, l'agenzia ha ridotto la superficie di attacco, ha migliorato i tempi di risposta agli incidenti e ha raggiunto la piena conformità alle normative di sicurezza federali. Questo caso dimostra l'efficacia dell'integrazione trasversale a più pilastri per trasformare un'architettura di sicurezza frammentata in un modello di sicurezza coerente e dinamico che supporta l'approccio Zero Trust.

Conclusione

La sicurezza Zero Trust non è più una semplice opzione. È ormai una necessità per proteggere le agenzie federali da minacce informatiche sempre più sofisticate. Implementando la microsegmentazione, la sicurezza delle API e rigorosi controlli delle identità, enti e agenzie federali possono ridurre drasticamente il rischio mantenendo la conformità ai requisiti federali di sicurezza informatica.

Akamai offre una suite completa di soluzioni Zero Trust, tra cui Akamai Guardicore Segmentation, Akamai API Security e Akamai Secure Internet Access Enterprise, per consentire alle agenzie di adottare un approccio proattivo e adattivo alla sicurezza. Grazie all'esperienza di Akamai, gli enti federali possono accelerare il percorso verso un approccio Zero Trust e garantire la resilienza della sicurezza a lungo termine.

È arrivato il momento di agire per gli enti federali. Integrando le soluzioni per la sicurezza di Akamai, le agenzie possono raggiungere la maturità Zero Trust, mitigare i rischi informatici e salvaguardare gli asset digitali più critici per il paese.

Contatta Akamai oggi stesso per ulteriori informazioni sulle nostre soluzioni complete per la sicurezza.

Le soluzioni per la sicurezza di Akamai proteggono le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o la customer experience. Grazie alla scalabilità della nostra piattaforma globale e alla sua capacità di individuare le minacce, possiamo lavorare con voi per prevenire, rilevare e mitigare le minacce informatiche e permettervi di rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X e LinkedIn. Data di pubblicazione: 04/25.