DESCRIZIONE DEL PRODOTTO AKAMAI

# Secure Internet Access ThreatAvert

## Protezione di importanti risorse di rete e identificazione del malware che danneggia gli utenti

I provider di servizi riconoscono che la sicurezza delle reti promuove il valore del brand perché influisce direttamente sulla soddisfazione degli utenti. Sono state sviluppate nuove minacce, perlopiù basate sul DNS, che mirano specificatamente all'infrastruttura DNS di importanza critica. I provider devono ripensare al modo in cui proteggere le risorse di rete e gli utenti, in particolare quando le minacce diventano più dinamiche e diversificate in un mondo in cui tutto è connesso.

Akamai Secure Internet Access ThreatAvert valuta le ricerche DNS in tempo reale per rilevare e interrompere le attività dannose. Secure Internet Access ThreatAvert mira alle minacce che provocano interruzioni o rallentamenti della rete, influiscono negativamente sull'experience dell'utente o minano altre protezioni di rete, tra cui:

- Attacchi DDoS basati su DNS che sovraccaricano i resolver con enormi volumi di query
- Malware bot che rubano preziosi dati personali o violano i dispositivi consumer
- Tunnel DNS che sottraggono servizi tramite il trasporto di altri protocolli all'interno del DNS

La soluzione Secure Internet Access ThreatAvert, basata sull'innovativo resolver DNS CacheServe di Akamai, si avvale dei feed sulle minacce dinamiche di Akamai. CacheServe rappresenta il massimo livello di affidabilità, grazie ad anni di investimenti profusi nell'ottimizzazione delle performance e nell'applicazione di numerosi miglioramenti software, per garantire resilienza e disponibilità anche nel caso di enormi picchi di traffico DNS. Creato dal team Data Science di Akamai, il team Threat Intelligence elabora più di cento miliardi di query DNS in live streaming provenienti da tutto il mondo ogni giorno.

### La sicurezza DNS risiede nei server DNS

Le query DNS costituiscono un indicatore significativo di attività dannose, perché la risoluzione dell'indirizzo di una risorsa dannosa (come server Command and Control, download di malware, sito di esfiltrazione, ecc.) rappresenta il primo passo per l'attivazione della maggior parte delle forme di questo tipo di attività. I resolver DNS rappresentano un luogo ideale per incorporare l'intelligence in grado di individuare le minacce, perché sono in grado di visualizzare tutte le query su un provider di rete. È pertanto possibile rilevare le attività dannose confrontando le query in entrata rispetto alle voci contenute negli elenchi delle minacce dinamiche.

### VANTAGGI PER IL BUSINESS

- Soluzione leggera e scalabile per milioni di utenti, supporta ogni dispositivo
- Data Science, come leader del settore, offre una straordinaria profondità e portata della copertura dalle minacce
- I feed sulle minacce aggiornati continuamente mantengono la protezione durante la modifica degli exploit
- I rapporti in tempo reale di facile lettura mostrano immediatamente lo stato delle minacce con un link per i dettagli
- Raccolta efficiente e gestione scalabile dei dati sulle minacce e sulla telemetria

Akamai

Secure Internet Access ThreatAvert offre scalabilità nel piano di controllo DNS con costi, impegno operativo e impatto sulla rete di gran lunga inferiori rispetto alle soluzioni dedicate di elaborazione dei pacchetti, che offrono scalabilità con il traffico del piano dati.

La soluzione è leggera ed efficiente e non comporta latenza aggiuntiva per il traffico di rete. Poiché è basata sulla rete, offre copertura per ogni dispositivo; inoltre, i client e gli host non richiedono installazione o aggiornamenti di software di sicurezza.

## Precisione, profondità e ampiezza della copertura dalle minacce di livello superiore

Gli sviluppatori di malware realizzano continue innovazioni per massimizzare il ritorno sugli investimenti dei loro exploit. Ciò significa che la maggior parte delle minacce viene accuratamente progettata per eludere il rilevamento e cambia rapidamente in modo da mantenere la propria efficacia. Anche la superficie di attacco si è moltiplicata e include oggi una sbalorditiva varietà di elementi IoT (Internet delle cose) connessi; di conseguenza, esiste una notevole diversità nei metodi utilizzati dagli autori degli attacchi per raggiungere i loro obiettivi.

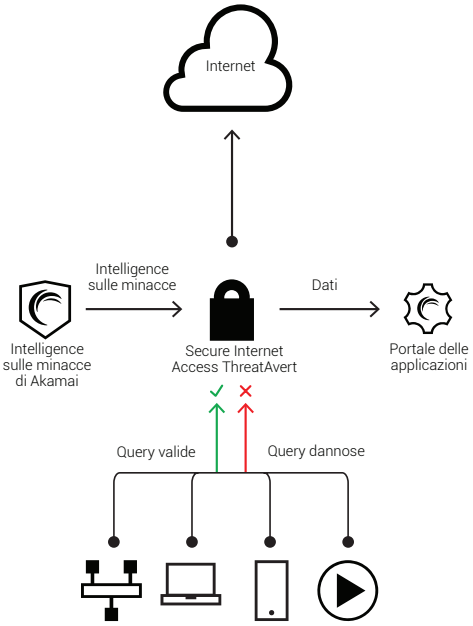
Riconoscendo la raffinatezza e la diversità del panorama delle minacce, il team Data Science di Akamai ha sviluppato, implementato e integrato sistemi chiave per analizzare le query DNS in live streaming. Il processo ingloba l'uso dei dati sulle minacce contenuti in elenchi di reputazione, honeypot e altre fonti di terze parti. Inoltre, la copertura dalle minacce, la precisione e l'agilità hanno raggiunto nuovi livelli di portata e profondità a seguito degli investimenti effettuati in:

- Algoritmi in attesa di brevetto per rilevare immediatamente un comportamento anomalo (come DNS-DDoS), correlare minacce eterogenee e identificare nuovi DGA (Domain Generation Algorithm) dei bot
- Tecniche avanzate per consentire automaticamente ai nomi di garantire una protezione costante delle query DNS "buone"
- Personale di ricerca con anni di competenze in materia di sicurezza e una profonda comprensione dei malware e dei dati DNS
- Rete mondiale e data center per l'elaborazione in tempo reale di flussi di dati live

## Le policy di precisione bloccano il traffico dannoso e proteggono il traffico legittimo

Le policy di precisione sono incorporate nell'intelligence sulle minacce di Akamai per gestire il traffico DNS indesiderato. Un set di funzioni ampio e completo consente un filtraggio minuzioso per individuare query dannose e proteggere (rispondere a) query legittime:

- È possibile applicare le policy di precisione alle query in entrata o alle risposte in uscita
- È possibile impostare filtri o limiti di velocità in base a IP, QTYPE, FQDN o molti altri parametri di query
- I filtri o i limiti di velocità possono utilizzare più parametri di query insieme a operatori logici: QTYPE E FQDN, IP E FQDN, ecc.




Il grande flusso di dati elaborato dagli esperti di Akamai offre un quadro completo delle attività dannose perpetrate tramite Internet, nonché degli attacchi localizzati.

- È possibile mettere a confronto i filtri o i limiti di velocità rispetto agli elenchi delle minacce dinamiche forniti dall'intelligence sulle minacce di Akamai o agli elenchi forniti dall'operatore
- È possibile combinare policy ed elenchi delle minacce: CORRISPONDENZA rispetto a BLOCKLIST e NON con ALLOWLIST
- Più azioni di policy determinano le modalità di gestione delle query: è possibile ignorarle, sintetizzare la risposta, rispondere con troncamento, NXD, NOERROR e molto altro ancora
- È possibile combinare e inserire le policy una nell'altra per renderle ancora più efficaci

È possibile anche configurare manualmente le policy di precisione, per affrontare problemi localizzati nella rete di un provider.

## Gestione dei dati scalabile, telemetria completa e generazione di rapporti

Secure Internet Access ThreatAvert incorpora un'architettura per la gestione dei dati basata su soluzioni aperte che sono state collaudate nelle reti più grandi al mondo, al fine di offrire l'eccellenza operativa su una vasta scala web e ad alte velocità. I dati in live streaming dei sistemi Secure Internet Access ThreatAvert a livello di rete vengono aggregati e resi disponibili per la generazione di rapporti (come descritto di seguito) e altri sistemi. L'architettura flessibile fornisce una disponibilità continua per favorire un'experience ininterrotta del cliente. È possibile utilizzare connettori opzionali per l'apertura di sistemi big data (Splunk, Hadoop) o applicazioni appositamente progettate per ricavare ulteriori informazioni operative, di sicurezza e aziendali.

I rapporti Secure Internet Access ThreatAvert offrono un'immediata valutazione dell'approccio in termini di sicurezza grazie ad un dashboard esecutivo che visualizza le query DNS bloccate, la larghezza di banda DNS di picco salvata, i principali malware presenti nella rete, gli utenti infetti ed eventuali aggiornamenti dell'intelligence sulle minacce. Un'ulteriore dashboard di sicurezza fornisce grafici contenenti dettagli su malware e DDoS. È, inoltre, possibile ottenere con un semplice clic livelli successivi di dettagli su malware e client infetti. È infine possibile creare dashboard e rapporti personalizzati in pochi minuti per visualizzare i dati sulla sicurezza in un formato definito dall'utente, al fine di soddisfare specifici requisiti operativi. I rapporti basati su tag consentono al personale addetto alle operazioni di configurare viste della propria