DESCRIZIONE DEL PRODOTTO AKAMAI

Account Protector

Tenete lontani i truffatori e conservate la fiducia dei clienti con la protezione dall'abuso degli account

Come è possibile riconoscere gli utenti legittimi dagli impostori? I vostri clienti si fidano di voi per distinguerli.

Man mano che le transazioni digitali e l'adozione delle nuove risorse digitali continuano a diffondersi sempre più, le conseguenze e i rischi associati all'abuso degli account sono più significativi che mai. L'abilità di espandere l'e-business e proteggere i clienti dipende dalla vostra capacità di mantenere la fiducia dei clienti in un ambiente in cui le tattiche delle frodi sono in continua evoluzione.

Un abuso correlato agli account, come un'apertura fraudolenta di account (anche nota come truffa del nuovo account) e un attacco per il controllo degli account (ATO), pone sfide e costi significativi per le aziende di tutti i settori. Gli account violati e fittizi possono avere gravi conseguenze finanziarie e sulla reputazione per le organizzazioni. Se un account viene compromesso, i criminali possono sfruttarlo liberamente, prosciugando le risorse economiche, effettuando transazioni fraudolente, disattivando le funzioni di sicurezza come l'MFA o rubando informazioni personali sensibili. È possibile usare, d'altro canto, gli account fittizi per trarre vantaggio da promozioni come buoni e versioni di prova gratuite, per inviare grandi quantità di messaggi SMS e per inondare le piattaforme con spam o contenuti inappropriati. L'impatto di questi attacchi è significativo e le aziende devono affrontare il rischio di compromettere la fiducia dei clienti, perdere milioni a causa delle frodi e vedersela con sanzioni normative e danni alla reputazione.

Akamai Account Protector

Account Protector è una soluzione di sicurezza progettata per prevenire l'abuso degli account in tutto il loro ciclo di vita, utilizzando l'apprendimento automatico e un significativo dataset di indicatori di rischio e attendibilità per stabilire la legittimità della richiesta di un utente. La soluzione analizza il comportamento degli utenti in tempo reale per identificare il minimo segnale di attività fraudolenta dalla creazione dell'account fino alla procedura di login e oltre. Se rileva un comportamento sospetto o anomalo, Account Protector offre varie opzioni di mitigazione immediata per mantenere un livello di user experience eccellente, ad esempio bloccando e intervenendo sull'edge, distribuendo sfide crittografiche e comportamentali, inviando contenuti alternativi e molto altro.

Vantaggi per le aziende

Aumento della fiducia: la vostra e quella dei vostri clienti
Scoprite quali interazioni sono legittime, riducete le criticità per gli utenti e proteggeteli dalle attività fraudolente.

Sviluppo di sistemi di protezione specifici per la vostra azienda
Sfruttate l'ottimizzazione automatica dei sistemi di rilevamento dei bot e la capacità di comprendere i profili della popolazione degli utenti in base alla loro modalità di interazione con il vostro sito.

Visibilità e informazioni dettagliate
Adottate le misure appropriate con la massima tranquillità sulla base di indicatori e segnali chiari.

Riduzione delle conseguenze legate alla mitigazione
Diminuite il consumo di finanze e risorse per indagare sugli account compromessi, sostituire le risorse rubate e molto altro.

Migliori decisioni sulle identità e sulla sicurezza basate sui dati
Integrate la soluzione con i sistemi di rilevamento delle frodi, gli strumenti SIEM e altre soluzioni di sicurezza per utilizzare i segnali di attendibilità e di rischio offerti da Account Protector al fine di migliorare l'accuratezza e ottimizzare gli investimenti effettuati in questi strumenti.

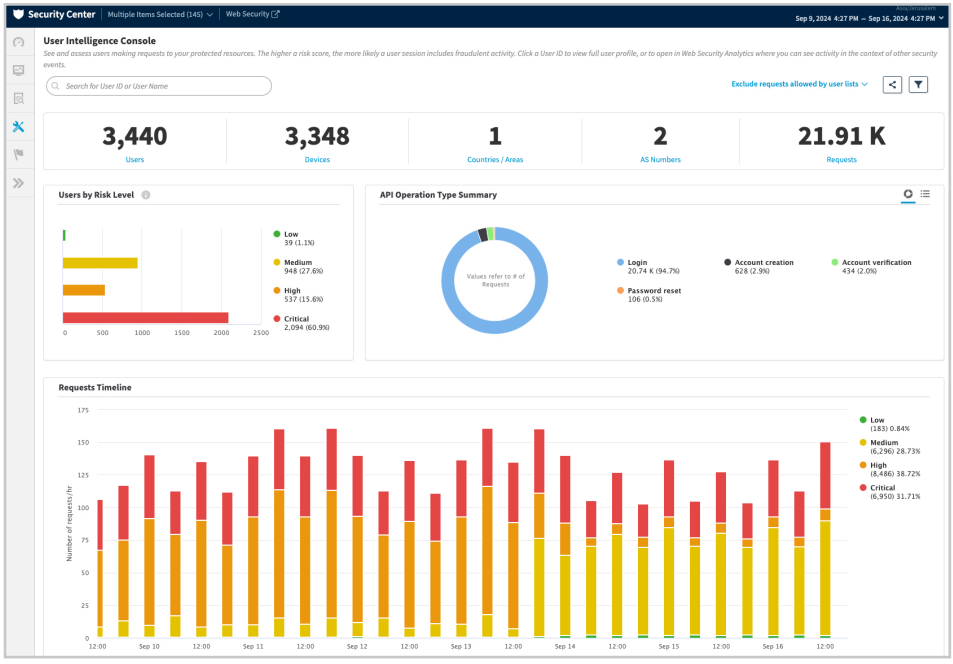
Una difesa olistica dall'abuso degli account

Proteggete gli account degli utenti dagli abusi per tutto il loro ciclo di vita, fornendo una protezione avanzata dall'abuso di apertura degli account, dagli attacchi per il controllo degli account e da altri schemi di attacco.

Abuso di apertura degli account: mitigate la creazione di account fittizi, che vengono utilizzati per trarre vantaggio da promozioni, inviare grandi quantità di messaggi SMS, provare i dati delle carte di credito rubati, sottrarre dati dagli inventari e molto altro.

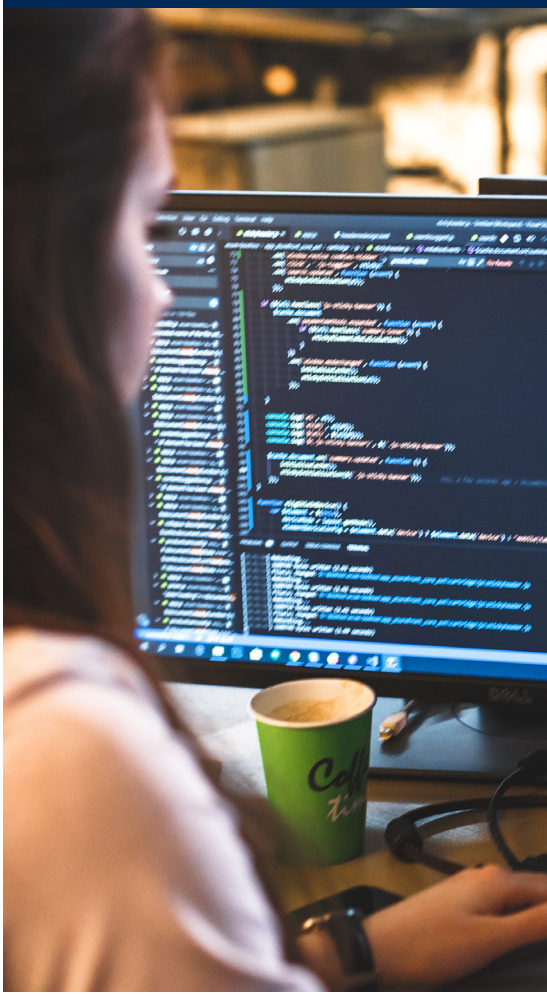
Attacchi per il controllo degli account: proteggetevi dai criminali che riescono ad accedere agli account dei clienti legittimi per sottrarre le loro risorse, rubare dati sensibili ed eseguire transazioni fraudolente.

Avanzati attacchi di bot dannosi: proteggete gli account utente dagli attacchi di credential stuffing, manipolazione dell'inventario e altri attacchi automatizzati spesso sferrati insieme all'abuso di apertura degli account o ad attacchi ATO per sottrarre beni preziosi, soldi o altre risorse di valore.



Protezione e fiducia delle user experience

Analizzate i rischi e fermate gli abusi in tempo reale, monitorando continuamente gli account durante il loro intero ciclo di vita alla ricerca di segnali di comportamenti sospetti non appena si verificano.



Funzionalità principali

Protezione completa del ciclo di vita degli account: identifica e analizza i rischi degli utenti in ogni fase, dalla creazione degli account alle attività di post-login, come aggiornamenti degli account, modifiche alle password e pagamenti.

Punteggio del rischio di una sessione utente in tempo reale: valuta i segnali di attendibilità e di rischio durante una sessione al fine di stabilire se una richiesta proviene dal legittimo utente dell'account o da un impostore.

Intelligence sugli indirizzi e-mail: analizza la sintassi di un indirizzo e-mail e l'uso anomalo di un messaggio e-mail per rilevare modelli dannosi.

Intelligence sui domini e-mail: valuta il modello delle attività provenienti dai singoli domini e-mail, inclusi i domini temporanei e l'eccessivo uso di un dominio e-mail.

Riconoscimento globale degli utenti attendibili: fornisce visibilità sui comportamenti degli utenti nella rete di Akamai per consentire di prendere decisioni più oculate sull'attendibilità degli accessi.

Profili comportamentali degli utenti: costruisce profili comportamentali degli utenti in base a posizioni, reti, dispositivi, indirizzi IP e tempi di attività osservati in precedenza per riconoscere gli utenti che tornano a visitare il vostro sito.

Profili della popolazione: aggrega i profili degli utenti dell'organizzazione in un soprainsieme, pertanto le varianti del comportamento possono essere anche confrontate con l'intera popolazione degli utenti per il rilevamento di eventuali anomalie.

Reputazione delle fonti: valuta la reputazione delle fonti sulla base delle attività dannose osservate in precedenza fra tutti i clienti Akamai, inclusi molti dei più grandi, trafficati e frequentati siti web a livello mondiale.

Indicatori: ciascuna richiesta viene valutata con indicatori generici, di rischio e attendibilità per stabilire il rischio di un abuso degli account. Gli indicatori vengono forniti insieme al punteggio di rischio finale e possono essere usati per eseguire analisi.

Rilevamento dei bot sofisticato: rileva accuratamente i bot sconosciuti dalla prima interazione, usando una varietà di modelli e tecniche di apprendimento automatico e di intelligenza artificiale (AI). Tali tecniche includono analisi telemetrica/comportamentale degli utenti, browser fingerprint, rilevamento automatizzato del browser, rilevamento delle anomalie HTTP, tasso di richieste elevato e altro ancora.

Analisi e generazione di rapporti: fornisce rapporti in tempo reale e cronologici. Potete analizzare le attività sui singoli endpoint, indagare su uno specifico utente, riesaminare gli utenti in base al loro livello di rischio e ottenere informazioni dettagliate.

Azioni di risposta avanzate: fornisce un'ampia gamma di azioni da poter applicare per fermare gli abusi, tra cui avviso, blocco, ritardo, distribuzione di sfide crittografiche e comportamentali, invio di contenuti alternativi e molto altro. Inoltre, le organizzazioni possono assegnare diverse azioni in base all'URL, al momento della giornata, alla posizione geografica, alla rete o alla percentuale di traffico.

Inserimento di intestazioni: invia informazioni sui rischi per gli utenti a scopo di analisi e mitigazione in tempo reale. Un'altra intestazione sulla richiesta viene inserita con informazioni sul punteggio di rischio dell'utente e sugli indicatori generici, di rischio e attendibilità che hanno contribuito a raggiungere quel determinato punteggio per eseguire ulteriori analisi e misure di mitigazione in tempo reale.

Automazione con apprendimento automatico: aggiorna automaticamente le caratteristiche e i comportamenti utilizzati per identificare i bot e le attività fraudolente dei criminali, dagli schemi di comportamento ai più recenti punteggi della reputazione nella piattaforma di Akamai.

Integrazione SIEM (opzionale): integra le informazioni sui rischi degli utenti negli strumenti SIEM per offrire una maggiore visibilità sulla sicurezza. Potete aumentare il valore dei vostri strumenti esistenti con le informazioni fornite da Account Protector.

Per ulteriori informazioni, contattate il vostro rappresentante Akamai oppure visitate il sito Akamai.com.