DESCRIZIONE DEL PRODOTTO AKAMAI

Client-Side Protection & Compliance

Proteggetevi dalle vulnerabilità JavaScript lato client e semplificate la conformità normativa

JavaScript è uno strumento essenziale per le moderne applicazioni web. Dall'ottimizzazione delle user experience al miglioramento delle funzionalità e delle performance, l'uso del linguaggio JavaScript proprietario e di terze parti è aumentato in modo esponenziale nel tempo. Sebbene il suo utilizzo presenti numerosi vantaggi, una supply chain digitale JavaScript può anche esporre i siti web ad attacchi lato client che mirano a sottrarre informazioni sensibili degli utenti finali dal browser, inclusi i dati delle carte di pagamento, tramite l'inserimento di codice dannoso.

Poiché questi attacchi non sono visibili dal lato server e aggirano le tradizionali misure di sicurezza, colpiscono facilmente le organizzazioni, che subiscono danni in termini di fiducia dei clienti e reputazione del brand e incorrono in pesanti sanzioni dovute all'inadempienza normativa e alla mancata conformità.

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance aiuta a evitare l'esfiltrazione dei dati degli utenti finali e protegge i siti web dalle minacce JavaScript. Questa soluzione è progettata per rilevare il comportamento di script dannosi e fornire ai team di sicurezza avvisi utili per mitigare le attività dannose in tempo reale.

Con funzionalità di conformità PCI DSS v4.0 appositamente progettate, Client-Side Protection & Compliance aiuta le organizzazioni a soddisfare i nuovi requisiti di sicurezza degli script e protegge i dati delle carte di pagamento dagli attacchi lato client. Potrete gestire facilmente l'inventario degli script della pagina di pagamento, semplificare il processo di controllo tramite un unico dashboard completo e ricevere avvisi PCI dedicati per rispondere rapidamente agli eventi correlati alla conformità.

Funzionalità principali

Protezione contro l'esfiltrazione dei dati sensibili lato client

I criminali informatici sono sempre alla ricerca dei dati sensibili dei vostri utenti finali. Sfruttando le vulnerabilità nelle supply chain JavaScript, gli utenti malintenzionati riescono a iniettare nei siti web un codice che permette di sottrarre i dati sensibili ed esfiltrarli per scopo fraudolento. Client-Side Protection & Compliance combina apprendimento automatico e punteggio euristico per analizzare il comportamento degli script in tempo reale al fine di rilevare attività dannose e risorse vulnerabili. Offre ai team di sicurezza avvisi immediatamente utilizzabili per attuare rapidamente una strategia di difesa contro gli attacchi lato client, come web skimming, Magecart e formjacking.

VANTAGGI PER LE AZIENDE

Rilevamento e protezione
Monitora il comportamento degli script nelle sessioni di utenti reali per rilevare attività sospette

Workflow PCI DSS v4.0
Aiuta a soddisfare i requisiti di sicurezza JavaScript 6.4.3 e 11.6.1

Avvisi in tempo reale Consente di mitigare immediatamente gli eventi ad alto rischio con avvisi utilizzabili

Visibilità lato client
Offre ampia visibilità della superficie di attacco lato client

Gestione delle policy
Regola il comportamento degli script e controlla l'esecuzione del runtime Javascript

Rilevamento delle vulnerabilità
Identifica le CVE (Common Vulnerabilities and Exposures) grazie al supporto dell'intelligence sulle minacce Akamai

Opzioni di distribuzione flessibili
Semplifica la distribuzione tramite Akamai Connected Cloud o direttamente sul server di origine

Akamai

Supporto dedicato per la conformità PCI DSS v4.0

I requisiti di sicurezza degli script 6.4.3 e 11.6.1 per il PCI DSS v4.0 impongono alle organizzazioni la necessità di proteggere i dati delle carte di pagamento dagli attacchi lato client e garantire la gestione degli script nelle pagine di pagamento. Client-Side Protection & Compliance monitora e cataloga tutti gli script sulle pagine di pagamento, garantendone l'integrità e autorizzandone l'uso. Fornisce giustificazioni predefinite e regole automatizzate per giustificare facilmente tutti gli script caricati. Inoltre, la soluzione monitora le modifiche alle intestazioni HTTP e alla protezione delle pagine di pagamento per evitarne la manomissione. Un dashboard completo e avvisi PCI dedicati consentono alle organizzazioni di rispondere rapidamente agli eventi correlati alla conformità e garantiscono la protezione dei dati delle carte di pagamento all'interno del browser. Grazie a queste funzionalità, i team di sicurezza e conformità possono ridurre il carico di lavoro del processo di controllo in ambito PCI (settore delle carte di pagamento) e semplificare rapidamente i workflow.

Ampia visibilità delle minacce JavaScript

Le tradizionali protezioni delle applicazioni web, come i firewall, si limitano a monitorare il traffico lato server e non offrono visibilità sulle attività eseguite sul lato client. Gli approcci basati su standard per la protezione da tali minacce, come le policy di sicurezza dei contenuti, sono difficili da gestire e offrono una protezione limitata contro i payload dannosi introdotti nella supply chain di script al di fuori del controllo degli operatori delle pagine web. Ciò crea un punto cieco per le organizzazioni, consentendo al codice dannoso di sfuggire al rilevamento per giorni, settimane o addirittura mesi e continuare a sottrarre dati sensibili. Client-Side Protection & Compliance offre una visione senza pari della superficie di attacco lato client del vostro sito web, inclusi il comportamento, le vulnerabilità, la portata e l'impatto di ogni script, gli accessi ai dati o le minacce poste.

Come funziona

Client-Side Protection & Compliance viene eseguito nel browser dell'utente finale per monitorare l'esecuzione degli script lato client su una pagina web protetta. Se si rilevano cambiamenti nel comportamento degli script, vengono impiegate tecniche di apprendimento automatico per valutare il rischio di possibili azioni non autorizzate o inappropriate. Informa i team di sicurezza in caso di eventi ad alto rischio, consentendo di analizzare e mitigare immediatamente le potenziali minacce.

Configurazione. Vengono inseriti semplici script in ogni pagina monitorata senza alcun impatto significativo sulle performance.

Monitoraggio e valutazione. I dati dell'attività JavaScript vengono raccolti dal browser web di un utente e monitorati. Vengono utilizzate tecniche di apprendimento automatico per valutare il rischio di azioni non autorizzate o inappropriate, se rilevate.

Avvisi. Vengono inviati avvisi in tempo reale con informazioni dettagliate per mitigare le minacce in caso di rilevamento di una minaccia o di un attacco attivo.

Mitigazione. Vengono immediatamente attuate procedure per impedire ai codici JavaScript dannosi di accedere ed esfiltrare i dati sensibili sulle pagine protette con un semplice clic.

Accelerate la conformità con i requisiti di sicurezza degli script per il PCI DSS v4.0

Integrità e autorizzazione degli script (6.4.3)

Garantite l'integrità e l'autorizzazione di tutti gli script caricati sulle pagine di pagamento protette.

Inventario e giustificazione degli script (6.4.3)

Monitorate e catalogate gli script caricati nelle pagine di pagamento protette. Giustificate rapidamente tutti gli script utilizzando giustificazioni predefinite e regole automatizzate.

Protezione delle pagine di pagamento (11.6.1)

Rilevate immediatamente le modifiche non autorizzate sulle pagine di pagamento e agite di conseguenza.

Dashboard intuitivo

Semplificate il processo di conformità e controllo PCI DSS v4.0 tramite un dashboard dedicato con informazioni dettagliate sulle attività correlate e gli avvisi per i requisiti di sicurezza degli script 6.4.3 e 11.6.1.

Avvisi PCI utilizzabili

Ricevete e registrate avvisi dettagliati per eventi relativi alla conformità PCI, inclusi script non autorizzati, esfiltrazione dei dati di pagamento e manomissione delle pagine di pagamento.

Per ulteriori informazioni, visitate la nostra pagina sul prodotto o contattate il team di vendita di Akamai.

 | Supporto | | Data di pubblicazione: 09/23