Akamai

WHITE PAPER

La strategia per proteggersi dai 10 principali rischi per la sicurezza delle API identificati dall'OWASP

Come Akamai può aiutarvi ad affrontare le minacce e le vulnerabilità delle API più comuni

I 10 principali rischi per la sicurezza delle API identificati dall'OWASP		Akamai può essere d'aiuto?
API1:2023	Violazione dell'autorizzazione a livello di oggetto	☑
API2:2023	Violazione dell'autenticazione	☑
API3:2023	Violazione dell'autorizzazione a livello della proprietà dell'oggetto	☑
API4:2023	Utilizzo delle risorse illimitato	☑
API5:2023	Violazione dell'autorizzazione a livello di funzione	☑
API6:2023	Accesso illimitato a flussi aziendali sensibili	☑
API7:2023	Falsificazione richieste lato server	☑
API8:2023	Errata configurazione della sicurezza	☑
API9:2023	Gestione dell'inventario inadeguata	☑
API10:2023	Utilizzo delle API non sicuro	☑

Le API sono il fulcro dei prodotti digitali, dei servizi e degli ambienti cloud di un'azienda. Inoltre, sono diventate lo standard per la creazione e la connessione delle applicazioni nel processo di migrazione di un numero sempre maggiore di organizzazioni all'architettura basata sui microservizi per lo sviluppo delle app. Tuttavia, il costante accesso delle API a dati e sistemi critici le rende capaci non solo di favorire i ricavi, ma anche di creare rischi per le operazioni aziendali.

Le API vulnerabili o non correttamente configurate sono prevalenti, facili da violare e spesso non protette. Inoltre, è sufficiente una sola API violata per riuscire a rubare milioni di dati.

Poiché il 78% delle organizzazioni afferma di aver riscontrato problemi di sicurezza delle API nel corso di un anno, è chiaro che la protezione delle API deve essere affrontata in modo prioritario. Tuttavia, la superficie di attacco delle API è diventata rapidamente un bersaglio allettante, molto più velocemente di quanto la maggior parte delle aziende non siano riuscite a capire i seguenti aspetti:

Rischi per le API

Metodi di attacco delle API

Funzionalità e controlli di sicurezza delle API

Che cosa comprende la superficie di attacco delle API? In breve, questa superficie è molto più ampia di quanto pensino molte organizzazioni. Il concetto tradizionale di API (come le API da macchina a macchina o quelle di terze parti) può e deve essere ampliato per includere i servizi di applicazioni mobili e web in quanto parte dell'architettura basata sui microservizi. In altre parole, una richiesta web nell'ambito dell'architettura è un'API che gestisce una chiamata (tra varie chiamate) a vari microservizi.

78%

Percentuale di organizzazioni che afferma di aver riscontrato problemi di sicurezza delle API in un anno. È chiaro che la protezione delle API deve essere affrontata in modo prioritario.

Il 5 giugno 2023, lo stimato OWASP (Open Worldwide Application Security Project) ha pubblicato il primo importante aggiornamento al suo iniziale elenco con i 10 rischi per la sicurezza delle API stilato nel 2019. L'elenco aggiornato descrive come ciascuna di queste chiamate API sia potenzialmente in grado di aprire falle nei sistemi di sicurezza e comportare rischi per la privacy, tra cui:

Convalida dei dati di bassa qualità

Errori di configurazione

Difetti di implementazione

Lacune di integrazione tra i componenti della sicurezza

Scoprite i principali rischi identificati dall'OWASP e come la soluzione Akamai API Security possa aiutarvi a mitigarli.

Il problema è che anche le organizzazioni che affermano di disporre di un inventario completo delle loro API presentano una grave lacuna:

solo **4 organizzazioni su 10** sanno quali delle loro API restituiscono dati sensibili quando vengono chiamate.

API1:2023 - Violazione dell'autorizzazione a livello di oggetto (BOLA)

Le vulnerabilità BOLA (Broken Object Level Authorization) si verificano quando l'autorizzazione di un client non è adeguatamente confermata per l'accesso a ID oggetto specifici. Questa vulnerabilità può fornire ai criminali una possibilità per accedere direttamente alle risorse desiderate, bypassando l'atteso workflow delle applicazioni e ottenendo un accesso non autorizzato ai dati sensibili. Le organizzazioni possono ridurre questo rischio evitando di affidarsi soltanto agli ID oggetto passati nelle loro richieste dai client. Al contrario, le organizzazioni possono utilizzare ID oggetto casuali a cui non è possibile risalire facilmente per garantire un'efficace verifica per ogni oggetto. Mascherare il vero ID degli oggetti, quando occorre, può fornire un ulteriore livello di sicurezza.

Il contributo di Akamai

Gli avanzati sistemi di sorveglianza di Akamai consentono di monitorare le minacce e generare avvisi quando si tentano di sfruttare le vulnerabilità BOLA al fine di garantire un'azione e un'attenzione immediate.

Akamai mitiga questo rischio tramite:

- L'identificazione dei tentativi di sfruttamento delle vulnerabilità BOLA
- La classificazione degli endpoint delle API suscettibili allo sfruttamento delle vulnerabilità BOLA in base agli input ricevuti (ad es., parametri numerabili), nonché le relazioni tra proprietà e oggetti delle API
- La generazione di avvisi quando si tenta o si riesce a sfruttare le vulnerabilità BOLA

API2:2023 - Violazione dell'autenticazione (BA)

La violazione dell'autenticazione si riferisce a vulnerabilità di vasta portata che si verificano nel processo di autenticazione, esponendo il sistema ai criminali, che possono sfruttare questi punti deboli per compromettere la protezione delle API. Di solito, i criminali che sfruttano le vulnerabilità di violazione dell'autenticazione (BA) riescono a manipolare le falle esistenti nel sistema, come password deboli o replay di sessione. Per proteggersi dalle vulnerabilità BA, le organizzazioni possono stabilire rigorosi meccanismi di autenticazione e gestione dei segreti, come solide policy per le password, nonché rotazione delle chiavi, firme di token e chiavi di crittografia complesse. Il rafforzamento di queste policy rigorose nelle organizzazioni può ridurre in modo significativo i rischi.

Il contributo di Akamai

Akamai rafforza la sicurezza delle API identificando e correggendo i punti deboli nell'autenticazione, contrastando gli attacchi automatizzati e inviando avvisi in modo proattivo quando si tenta di sfruttare una vulnerabilità.

Akamai mitiga questo rischio tramite:

- L'identificazione degli endpoint delle API che non richiedono autenticazione o non seguono best practice per l'autenticazione, come firme di token o chiavi di crittografia deboli e l'accettazione dei token di autenticazione scaduti
- La protezione da attacchi di credential stuffing o al dizionario tramite le nostre funzionalità di gestione dei bot
- La gestione dell'autorizzazione dei token JWT (JSON Web Token) con firme di token complesse tramite le funzionalità della nostra soluzione API Gateway
- La generazione di avvisi quando si tenta di sfruttare le vulnerabilità BUA

API3:2023 - Violazione dell'autorizzazione a livello della proprietà dell'oggetto (BOPLA)

La BOPLA (Broken Object Property Level Authorization) è una falla nella sicurezza in cui un endpoint delle API espone inutilmente più proprietà di dati di quanto non sia necessario per svolgere la propria funzione, trascurando il principio del privilegio minimo.

Questa falla può fornire inavvertitamente ai criminali una quantità eccessiva di dati che, a loro volta, possono usarla per rilevare altre vulnerabilità o per scovare dati sensibili, inclusa la possibilità, da parte di utenti non autorizzati, di manipolare proprietà che non includono un accesso a livello di amministratore, il che può compromettere ulteriormente l'integrità del sistema. Per garantire la sicurezza e impedire ai criminali di ottenere o manipolare un surplus di informazioni, è fondamentale fornire appropriati livelli di accesso e di esposizione dei dati al fine di evitare che potenziali criminali riescano a sfruttare queste falle.

Il contributo di Akamai

Sfruttando le tattiche complete di Akamai, le aziende possono mitigare i rischi correlati alle vulnerabilità BOPLA identificando e catalogando gli endpoint API e le loro proprietà associate.

Akamai mitiga questo rischio tramite:

- L'identificazione e l'etichettatura di tutti gli endpoint e le proprietà API esposte, come le informazioni di identificazione personale (PII)
- L'identificazione di endpoint, oggetti e proprietà delle API ombra o non documentate, nonché delle proprietà anomale
- L'applicazione di policy di sicurezza su proprietà e parametri accettabili e definiti per garantire l'integrità dei dati
- L'applicazione di policy di sicurezza basata sulle specifiche OpenAPI/Swagger che consentono solo ad endpoint e a metodi delle API ben definiti di accedere alle proprietà e agli oggetti delle API
- La generazione di avvisi quando si tenta di sfruttare le vulnerabilità BOPLA

API4:2023 - Utilizzo delle risorse illimitato

Si tratta di un tipo di vulnerabilità (spesso definito "esaurimento delle risorse API") in cui le API non limitano il numero di richieste inviate o il volume dei dati restituiti entro un certo periodo di tempo. Questa falla può consentire l'accesso ai criminali che cercano di sferrare attacchi DoS (Denial-of-Service), rendendo il sistema non disponibile per gli utenti legittimi. Questi tipi di sfruttamento possono influire gravemente sulle attività aziendali, determinando la mancata disponibilità dei servizi, l'insoddisfazione dei clienti e la potenziale perdita di ricavi, a seconda della lunghezza e dell'ampiezza dell'interruzione. È fondamentale implementare le misure necessarie per limitare la velocità della richieste API e le dimensioni dei dati restituiti per impedire la perdita dei servizi.

Il contributo di Akamai

Akamai protegge le API dalla minaccia di un utilizzo delle risorse illimitato:

- Identificando gli endpoint a rischio e fornendo avvisi in tempo reale sui tentativi di attacchi volumetrici
- Individuando errori eccessivi, tentativi di accesso o comportamenti atipici che indicano un rischio

Akamai mitiga questo rischio tramite:

- L'identificazione degli endpoint delle API che non dispongono di limiti della velocità oppure stanno subendo attacchi di credential stuffing o ai dizionari volumetrici di grandi dimensioni
- L'avvio di workflow per rallentare o bloccare gli attacchi volumetrici
- La generazione di avvisi quando si tenta di sferrare attacchi volumetrici

API5:2023 - Violazione dell'autorizzazione a livello di funzione (BFLA)

La violazione dell'autorizzazione a livello di funzione (BFLA) si può verificare quando i modelli di controllo degli accessi per gli endpoint delle API vengono implementati in modo errato. Metodi di controllo degli accessi obsoleti o non corretti potrebbero non riuscire a restringere in modo adeguato gli accessi non autorizzati, consentendo ai criminali di accedere alle informazioni sensibili o al sistema nel complesso. Per mitigare questo rischio, le organizzazioni possono adottare il principio del privilegio minimo, garantendo che tutte le funzioni, specialmente quelle amministrative, siano accessibili solo agli utenti con le autorizzazioni appropriate.

Il contributo di Akamai

Monitorando le tempistiche dei comportamenti, applicando policy di sicurezza alle funzioni sensibili, gestendo la rotazione e la revoca delle chiavi e avvisando tempestivamente in caso di tentativi sospetti, Akamai può aiutare a rafforzare la strategia di prevenzione e risposta alle vulnerabilità BFLA delle organizzazioni.

Akamai mitiga questo rischio tramite:

- L'identificazione delle tempistiche dei comportamenti sull'accesso agli endpoint delle API attraverso l'acquisizione di utenti, chiavi API, token di accesso, ID di sessione, ecc.
- L'applicazione della rotazione delle chiavi o della revoca delle chiavi esposte tramite Akamai API Gateway
- La generazione di avvisi quando si tenta di accedere in modo sospetto alle funzioni amministrative

API6:2023 - Accesso illimitato a flussi aziendali sensibili

Questo rischio si verifica quando un'API espone operazioni di importanza critica, come la logica aziendale, senza un adeguato controllo sugli accessi, il che conduce allo sfruttamento delle vulnerabilità e ad accessi non autorizzati, causando un notevole danno all'organizzazione. Lo sfruttamento, di solito, richiede la comprensione del modello aziendale supportato dalle API, l'identificazione dei flussi aziendali sensibili e lo sfruttamento delle falle presenti in questi flussi, il che, ad esempio, può impedire ad utenti legittimi di acquistare un prodotto.

Il contributo di Akamai

Proteggete la vostra azienda con le soluzioni complete per la protezione delle API di Akamai, che offrono funzionalità di identificazione degli endpoint sensibili, avvisi in tempo reale in caso di sfruttamento delle vulnerabilità e consulenza di esperti per proteggere le operazioni e i dati di importanza critica.

Akamai mitiga questo rischio tramite:

- L'identificazione degli endpoint delle API, come flussi di pagamenti o endpoint che gestiscono le PII
- La generazione di avvisi quando si verificano potenziali tentativi di sfruttamento, dall'esfiltrazione alla manipolazione dei dati fino ai tentativi sospetti condotti su questi endpoint delle API sensibili

API7:2023 - Falsificazione richiesta lato server (SSRF)

Una vulnerabilità di questo tipo permette a un criminale di indurre l'applicazione lato server a inviare richieste HTTPS a un dominio arbitrario da lui scelto. In un attacco SSRF tipico, il criminale inganna il server effettuando una richiesta alle risorse interne, bypassando di conseguenza i firewall e ottenendo l'accesso ai servizi interni, il che può condurre all'esposizione dei dati o all'esecuzione di codice remoto. Per mitigare questo rischio, è fondamentale verificare, filtrare o ripulire gli input dell'utente e limitare le connessioni in uscita che il server può stabilire per far sì che possa comunicare solo con i servizi più importanti.

Il contributo di Akamai

Rafforzate il vostro sistema di sicurezza con Akamai, fornendo funzionalità di rilevamento delle anomalie in connessioni API affidabili, un'efficace gestione delle chiavi e notifiche immediate in caso di tentativi di sfruttamento delle vulnerabilità SSRF.

Akamai mitiga questo rischio tramite:

- L'applicazione di policy di protezione delle applicazioni web e delle API per contrastare gli attacchi SSRF
- L'applicazione della rotazione o della revoca delle chiavi esposte tramite API Gateway

API8:2023 - Errata configurazione della sicurezza

Si tratta di un'errata configurazione dei controlli di sicurezza, che può rendere un sistema vulnerabile agli attacchi e può includere configurazioni predefinite non sicure, configurazioni incomplete o ad hoc, storage sul cloud aperto, intestazioni HTTP(S) non correttamente configurate e messaggi di errore dettagliati contenenti informazioni sensibili. Per mitigare questi rischi, è vitale per le organizzazioni assicurarsi di aver configurato correttamente i propri controlli di sicurezza in tutti gli aspetti delle applicazioni e delle API che utilizzano, inclusi gli aggiornamenti regolari, i test accurati e il monitoraggio continuo eseguiti per identificare e correggere tempestivamente eventuali errori di configurazioni.

Il contributo di Akamai

Migliorate il livello delle vostre informazioni: Akamai vi aiuta ad identificare gli endpoint delle API ombra, non autorizzate o zombie, ad adottare le appropriate best practice di sicurezza, ad effettuare una solida implementazione dei protocolli HTTPS e a ricevere avvisi immediati in caso di errori di configurazione del sistema di sicurezza.

Akamai mitiga questo rischio tramite:

- L'identificazione degli endpoint delle API ombra che possono rendere vulnerabili gli ambienti di basso profilo (ad es., gli ambienti di test e staging)
- L'identificazione e l'associazione di endpoint, oggetti e proprietà delle API in base alle best practice e agli standard di configurazione della sicurezza
- L'applicazione di policy di sicurezza tramite le best practice di sicurezza delle API, come richieste e risposte HTTPS con formato corretto, la configurazione o la rimozione di intestazioni HTTP corrette, nonché il controllo completo delle intestazioni Cache-Control e CORS (Cross-Origin Resource Sharing)
- L'applicazione dell'appropriata implementazione dei protocolli HTTPS tramite SSL/TLS, incluse suite di crittografia corrette e sicure
- La generazione di avvisi in caso di errori di configurazione o di mancata conformità agli standard e alle best practice di sicurezza delle API

API9:2023 - Gestione dell'inventario inadeguata

Questo rischio rappresenta una sfida per tutte le organizzazioni che si occupano della gestione delle API. Le soluzioni per la sicurezza delle API possono proteggere le API note, ma le API sconosciute, comprese le API ombra, possono restare prive di patch e, quindi, vulnerabili agli attacchi. Tutto ciò può condurre a componenti obsoleti, pagine o API inutilizzate e un'esposizione non necessaria di informazioni sensibili. La presenza di servizi non gestiti può rendere i sistemi vulnerabili alle minacce, nel qual caso i criminali possono potenzialmente accedere ai dati sensibili o, persino, al server tramite API sconosciute, che sono connesse allo stesso database. I controlli degli accessi e le verifiche regolari sono essenziali per evitare costanti cambiamenti dei componenti che costituiscono i servizi di un'organizzazione.

Il contributo di Akamai

Akamai supervisiona continuamente il traffico delle API per aiutare a scoprire gli endpoint delle API nascoste e le API con potenziali rischi, fornendo alle organizzazioni un'archiviazione sicura dei dati, avanzate analisi delle minacce e avvisi immediati in caso di potenziali tentativi di sfruttamento.

Akamai mitiga questo rischio tramite:

- Il monitoraggio continuo del traffico delle API esposte che fluisce nei vostri ambienti, inclusi gli endpoint delle API nord-sud che prendono di mira le API pubblicamente accessibili e gli endpoint delle API interne est-ovest
- L'identificazione degli endpoint delle API ombra che possono rendere vulnerabili gli ambienti di basso profilo (ad es., gli ambienti di test e staging) o versioni di API obsolete e/o non documentate
- La creazione di un inventario delle API aggiornato sulla base della classificazione dei dati e del punteggio di rischio
- La generazione di avvisi quando si verificano potenziali tentativi di sfruttamento, dall'esfiltrazione alla manipolazione dei dati fino ai tentativi sospetti condotti su questi endpoint delle API sensibili

API10:2023 - Utilizzo delle API non sicuro

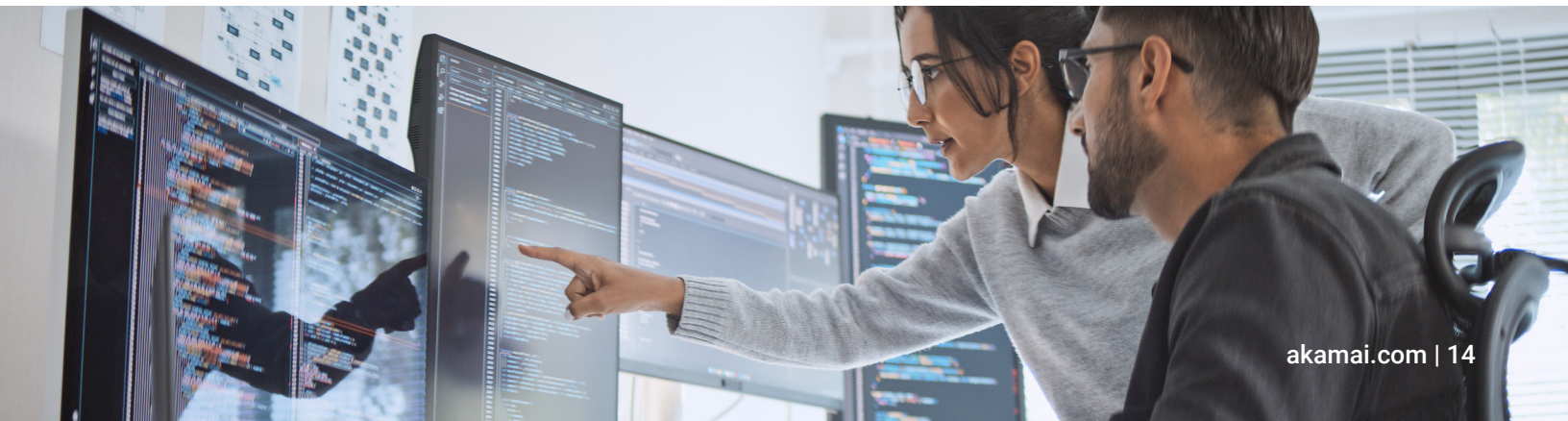
Si tratta dei rischi associati all'utilizzo delle API di terze parti, senza aver prima messo in atto misure di sicurezza adeguate. Per ampliare i loro servizi e le loro funzionalità, le organizzazioni si basano sempre più su API di terze parti, che, pertanto, vengono spesso considerate affidabili di default. Questo approccio può condurre, però, a significative vulnerabilità nel sistema di sicurezza. La mancata implementazione di appropriate procedure di crittografia, convalida e integrità dei dati, nonché limiti all'utilizzo delle risorse, possono esporre le organizzazioni a vulnerabilità significative. Per mitigare questi rischi, le organizzazioni possono implementare la crittografia a tutti i dati trasmessi tramite la rete, convalidare e verificare l'integrità di tutti i dati immessi e impostare limiti ragionevoli per l'utilizzo delle risorse.

Il contributo di Akamai

Proteggete costantemente i vostri sistemi monitorando e convalidando i vostri servizi per garantire la sicurezza con il monitoraggio, la generazione di avvisi e la consulenza di Akamai.

Akamai mitiga questo rischio tramite:

- Il monitoraggio continuo del traffico di tutte le API esposte che fluisce nei vostri ambienti, incluse le API est-ovest e in uscita che facilitano le integrazioni B2B (da azienda ad azienda) e/o di terze parti
- La generazione di avvisi quando si verificano potenziali tentativi di sfruttamento, dall'esfiltrazione alla manipolazione dei dati fino ai tentativi sospetti condotti su questi endpoint delle API sensibili
- L'applicazione di policy di protezione delle applicazioni web e delle API per contrastare una serie di attacchi alle API raccolti in gruppi di attacco



Altri rischi per la sicurezza identificati dall'OWASP

L'edizione 2023 dell'elenco OWASP con i 10 principali rischi per la sicurezza delle API è stato il primo importante aggiornamento a questo documento, che, pubblicato inizialmente nel 2019, includeva altri rischi per la sicurezza, come gli attacchi di tipo injection, ancora rilevanti nel panorama dei giorni nostri.

Akamai può aiutare a mitigare questi rischi alla sicurezza tramite:

- L'identificazione degli endpoint delle API vulnerabili agli attacchi di tipo injection e dei tentativi di sferrare attacchi di questo tipo mediante l'associazione di firme e il rilevamento di eventuali anomalie
- L'applicazione di policy di sicurezza tramite l'ispezione JSON e XML delle richieste di API e la scansione di vari attacchi di tipo injection, come gli attacchi SQLi, XSS, CMDi, RFI e LFI
- La generazione di avvisi quando si tenta di sfruttare le vulnerabilità agli attacchi di tipo injection

Inoltre, l'OWASP ha pubblicato altri elenchi simili, come l'elenco con i 10 principali rischi per la sicurezza delle applicazioni web. La gamma delle soluzioni per la sicurezza di Akamai può aiutarvi a mitigare anche questi rischi per la sicurezza.

Siamo qui per aiutarvi!

Le organizzazioni e i loro fornitori dei servizi di sicurezza devono lavorare a stretto contatto, sincronizzando persone, processi e tecnologie, al fine di costituire una solida difesa contro i rischi per la sicurezza descritti nelle 10 principali vulnerabilità per la sicurezza delle API riportate nell'elenco OWASP (Open Web Application Security Project).

Akamai offre soluzioni per la sicurezza leader del settore, esperti altamente competenti e una piattaforma che raccoglie informazioni da milioni di attacchi alle applicazioni web e alle API, miliardi di richieste di bot e migliaia di miliardi di richieste API ogni giorno.

Le soluzioni per la sicurezza delle applicazioni web e delle API di Akamai vi aiuteranno a proteggere la vostra organizzazione dalle forme più avanzate di attacchi alle applicazioni web, attacchi DDoS e basati sulle API. Inoltre, Akamai Managed Security Service fornisce funzioni di monitoraggio 24/7, gestione della sicurezza e mitigazione delle minacce.

Per maggiori informazioni relative alla gamma di prodotti per la sicurezza di Akamai, potete consultare il nostro sito web. Se desiderate discutere ed esplorare più nel dettaglio il modo con cui possiamo collaborare per creare la migliore protezione per la vostra azienda, contattate il vostro rappresentante vendite Akamai oggi stesso.

Akamai Security protegge le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo prevenire, rilevare e mitigare le minacce informatiche in ambienti ransomware affinché voi possiate 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 (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 09/24.