Akamai

WHITE PAPER

10 funzionalità critiche di rilevamento e risposta alle minacce delle API

Evoluzione della strategia di sicurezza delle API

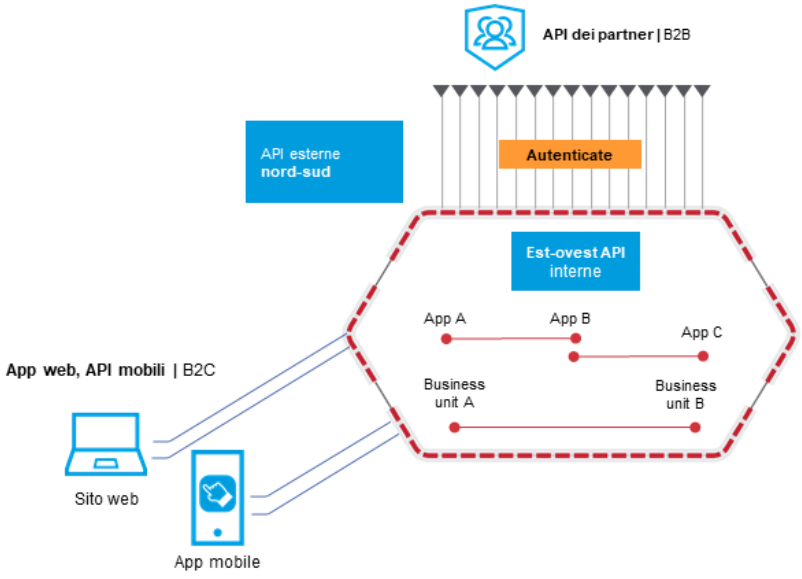
Introduzione

Le API sono elementi fondamentali per promuovere l'innovazione e le applicazioni B2B (da azienda ad azienda) e B2C (da azienda a consumatore) rappresentano la chiave per una trasformazione di successo. Ne consegue che è essenziale proteggere le comunicazioni critiche, spesso sensibili, sia internamente, tra i microservizi, che esternamente, tra clienti e partner. Ormai, nella maggior parte dei casi, le organizzazioni sanno che è necessario adottare una solida strategia di protezione delle applicazioni per ottenere risultati di business a lungo termine. Per questo motivo si avvalgono di tecnologie di sicurezza, quali le piattaforme WAAP (Web Application and API Protection), le funzionalità e i prodotti per la sicurezza nel cloud e gli strumenti per i test di sicurezza, volte a ridurre i rischi legati alla sicurezza delle applicazioni. È importante capire come si sono evoluti gli attacchi e in che modo tentano di eludere le piattaforme WAAP e di colpire le API delle organizzazioni. È il momento di adeguare la strategia di sicurezza delle API per prevenire queste minacce.

In che modo le attività di rilevamento e risposta si inseriscono in una strategia di protezione delle API?

Negli ultimi anni, le organizzazioni hanno creato molti più canali API che interfacce per applicazioni web e queste API includono volumi crescenti di dati e logiche aziendali essenziali. Le API hanno cambiato il modo di operare delle aziende poiché assicurano un maggior numero di casi di utilizzo, accelerano i cambiamenti, includono più dati sensibili e sono aperte a più utenti.

Qual è il vostro panorama delle API?



Benché la maggior parte delle categorie di prodotti per la sicurezza in qualche modo supporti le API per via della loro crescente diffusione, queste ultime rimangono una classe di risorse distinta e possono addirittura sembrare una risorsa diversa nell'ambito di determinati quadri di conformità. Aggiungere funzionalità di protezione dalle minacce alle API a un prodotto di sicurezza esistente, ad esempio una piattaforma WAAP, non risolverà le nuove sfide introdotte dalle risorse API. Le organizzazioni di sicurezza devono considerare le API come una classe di risorse separata e riconoscere le funzionalità critiche in grado di proteggerle totalmente e su vasta scala.

Iniziamo con una panoramica di come sono cambiati i criteri di protezione delle API per rispondere alle minacce emergenti. In passato, se un'organizzazione aveva un inventario completo delle proprie API e una solida piattaforma WAAP, poteva considerarsi sufficientemente protetta delle minacce alle API. Oggi, gli attacchi sono mirati alle API delle organizzazioni e delle organizzazioni partner e sono progettati per aggirare la protezione WAAP.

Ad esempio, alcune forme di violazione provengono da clienti e partner ai quali sono state concesse le credenziali API ma scelgono di utilizzarle in modo non autorizzato. Esistono anche metodi per dirottare le credenziali API o i token di sicurezza apparentemente legittimi. Le vulnerabilità nascoste nelle implementazioni dei client API sono un altro vettore di attacco che i malintenzionati possono sfruttare per violare le API in modi non rilevabili dagli strumenti di sicurezza tradizionali.

La buona notizia è che le funzionalità critiche necessarie per proteggere le API dalle tendenze emergenti, in particolare le tecnologie di rilevamento e risposta, sono già disponibili su larga scala. Le pagine seguenti forniscono una descrizione dettagliata delle funzionalità che rendono queste piattaforme efficaci contro le minacce alle API in continua evoluzione.

Funzionalità critica n. 1
Protezione indipendente dalla piattaforma

Generalmente, i servizi delle API sono implementati da diversi gruppi all'interno di un'organizzazione, spesso attraverso molteplici piattaforme e tecnologie. Alcune API possono essere, ad esempio, implementate on-premise mentre altre possono essere eseguite nel cloud pubblico. Inoltre, possono esistere tecnologie intermedie, quali proxy inversi, gateway API, Web Application Firewall (WAF) e reti per la distribuzione dei contenuti (CDN), che ostacolano la visibilità delle API.

La capacità di accedere ai dati sulle attività delle API da ciascuna di queste tecnologie è fondamentale. Un approccio di protezione indipendente dalla piattaforma garantisce alla vostra organizzazione un quadro sempre completo di tutte le attività delle API, indipendentemente dai dettagli di implementazione o dall'infrastruttura in uso. In questo modo si assicura la copertura per:

- Tutti i reparti, le aziende acquisite e gli ambienti
- Le API autorizzate e le API ombra, indipendentemente dal fatto che utilizzino o meno il gateway API
- Una visibilità estesa e non limitata alle API nord-sud, ma in grado di includere le API pubbliche, le API dei partner e le API interne est-ovest

L'ampia visibilità della piattaforma proteggerà la vostra organizzazione dalle minacce interne e dall'abuso delle API da parte delle organizzazioni partner, oltre che dai rischi provenienti da autori di minacce esterni.

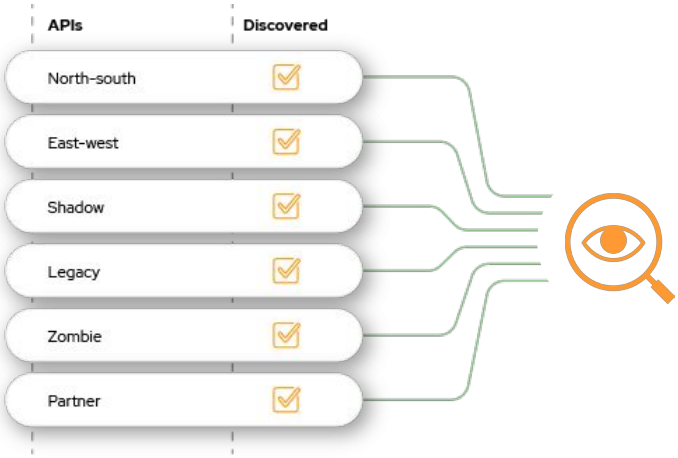
Funzionalità critica n. 2
Rilevamento continuo delle API e gestione del sistema

Un inventario completo e sempre aggiornato di tutte le API in uso nell'organizzazione è alla base di ogni strategia di protezione delle API. Ciò è vero per il semplice motivo che un'organizzazione non è in grado di proteggere elementi che non sa di avere nella propria infrastruttura. Molte aziende di prodotti per la sicurezza affermano di poter eseguire rilevamenti efficaci delle API, ma in realtà tali prodotti si limitano a un'operatività on-demand o giorno per giorno. È invece importante assicurarsi che le funzionalità di rilevamento delle API includano:

- Il rilevamento automatico e continuo delle API, 24 ore su 24, incluso il rilevamento delle API utilizzate una sola volta (il rilevamento on-demand o giorno per giorno non è sufficiente)
- Il rilevamento di tutte le API nelle diverse tecnologie e infrastrutture in uso
- Il rilevamento delle API appena distribuite e il confronto con le API ben documentate, per identificare le API ombra
- La valutazione del rischio di ciascun servizio ed endpoint delle API
- Il rilevamento dei casi noti di vulnerabilità delle API, come quelle descritte nell'elenco OWASP dei 10 principali rischi

Migliore visibilità

Non perdete più di vista l'inventario delle vostre API

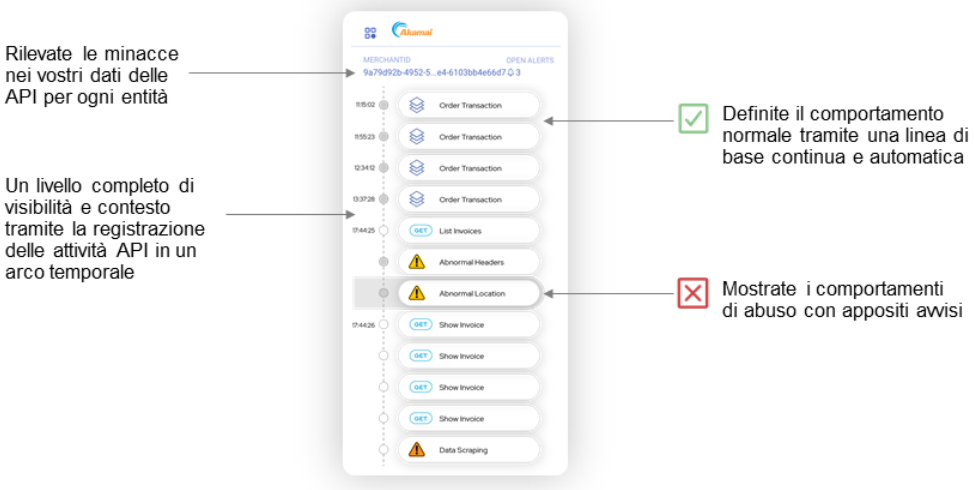


Funzionalità critica n. 3
Visualizzazione del comportamento delle API

La capacità di visualizzare ed esaminare il comportamento effettivo delle API (chiamate API) rappresenta una funzionalità fondamentale per una piattaforma di sicurezza. Questa funzionalità è necessaria per consentire agli esperti dei reparti di sicurezza, sviluppo e operatività di visualizzare e comprendere le modalità di utilizzo o abuso delle API, affinché possano garantire la comunicazione tra team e analizzare i vari casi. Alcune delle funzionalità di visualizzazione più importanti sono:

- **Indagine:** qualsiasi avviso deve includere la possibilità di analizzare l'attività dell'API originale, chiamata per chiamata, al fine di identificare il trigger specifico per l'avviso.
- **Ricerca delle minacce:** i dati cronologici devono estendersi ad almeno 30 giorni, con la possibilità di visualizzare tutte le attività delle API ed eseguire query per intervalli temporali e chiamate, oltre gli avvisi specifici. Questa funzionalità contribuisce anche a garantire la conformità ai requisiti del settore.
- **Fedeltà e arricchimento dei dati:** per ogni chiamata API, deve essere possibile sapere chi è l'utente, quale operazione ha utilizzato, a quali record ha avuto accesso o quali ha manipolato, quali intestazioni e parametri sono stati utilizzati, ecc.
- **Privacy dei dati:** sebbene la fedeltà dei dati sia importante, è necessario evitare che i dati sensibili siano archiviati. Bisogna quindi adottare un processo di tokenizzazione che preservi la ricchezza dei dati senza attivare l'archiviazione di quelli sensibili.
- **Visualizzazione della cronologia degli eventi:** gli utenti devono poter ricevere una vista che faciliti la navigazione tra le sequenze delle attività.

Rilevamento delle minacce tramite l'analisi comportamentale



Funzionalità critica n. 4
Tracciamento di più entità utente

Comprendere l'entità ed essere in grado di vedere le attività delle API correlate fornisce un contesto utile per identificare possibili usi o abusi, pertanto è fondamentale che la piattaforma di protezione abbia la capacità di monitorare singolarmente ciascuna entità. In questo modo si ottiene un contesto specifico e personalizzato, poiché quello che potrebbe essere considerato normale da alcuni utenti può rappresentare un segnale di abuso per altri. La capacità di visualizzare le attività di ciascuna entità nella cronologia degli eventi fornisce una visibilità e una comprensione vitali. Ad esempio:

Attività API	Partecipanti	Entità	Entità del processo aziendale
Esempi	Utenti interni, partner B2B (da azienda ad azienda), utenti esterni	Indirizzo IP, token API, ID commerciante, ID sessione, ID tenant	ID pagamento, ID fattura

Funzionalità critica n. 5
Copertura B2B (da azienda ad azienda) e API est-ovest

Il maggiore ambito di crescita nell'utilizzo delle API è rappresentato dai casi di utilizzo B2B (da azienda ad azienda) per utenti interni ed esterni. I sistemi di sicurezza devono difendere le API B2B da macchina a macchina, compresi il traffico nord-sud (utenti esterni) ed est-ovest (utenti interni).

Benché le applicazioni web B2C (da azienda a consumatore) beneficino della protezione dalle piattaforme WAAP e WAF, alcune attività più sensibili, come quelle delle API interne est-ovest o delle applicazioni proprietarie esposte ai partner tramite le API B2B (da azienda ad azienda), possono comunque essere compromesse.

Spesso, se un utente è autenticato sull'API di un partner B2B (da azienda ad azienda), viene considerato sicuro e non è sottoposto a ulteriore monitoraggio. Ciò determina una vulnerabilità critica nella strategia di sicurezza delle API di molte organizzazioni. Per fornire un quadro completo delle attività delle API e dell'esteso panorama delle minacce, le organizzazioni devono adottare un approccio che assicuri visibilità, osservabilità e monitoraggio, efficaci per tutti i casi di utilizzo.

Funzionalità critica n. 6
Analisi comportamentale e rilevamento

Non è possibile rilevare le sofisticate minacce alle API analizzando le singole chiamate API, o perfino le singole sessioni. Il rilevamento e la risposta alle minacce delle API richiedono una comprensione approfondita dei contesti comportamentali. Per sapere se il comportamento di un'API è anomalo, evento che indica che potrebbe essere compromessa, è necessario analizzare il suo impiego sul lungo periodo. La tecnica dell'analisi comportamentale identifica uno standard normale e monitora costantemente il comportamento per rilevare eventuali anomalie.

Le risorse di archiviazione ed elaborazione necessarie per eseguire tale analisi rendono poco pratica la delivery, poiché utilizzano strumenti di sicurezza delle API on-premise e vincolati dalle dimensioni. Le soluzioni EDR e XDR sono state pionieristiche e hanno dimostrato che è necessario disporre di un'architettura basata su SaaS (Software-as-a-Service) per eseguire analisi comportamentali significative. La potenza e le dimensioni del cloud consentono l'archiviazione dei dati nel tempo e permettono di eseguire analisi approfondite attraverso cui determinare quale sia il normale comportamento degli utenti. Un approccio SaaS offre altri vantaggi, tra cui un'implementazione più rapida e semplice, nonché una maggiore scalabilità ed elasticità commisurate all'aumento dell'utilizzo delle API.

Funzionalità critica n. 7
Avvisi significativi con contesto

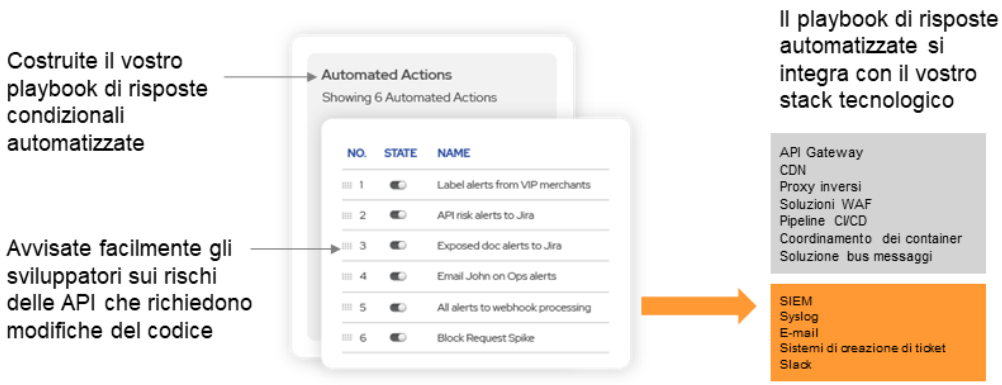
Quando un'organizzazione ha visibilità su tutte le attività delle API e le analisi comportamentali, gli avvisi acquisiscono maggiore significato. Le organizzazioni possono eliminare la necessità di anticipare ogni possibile attacco, rendendo più astratto l'approccio al monitoraggio della sicurezza. La definizione di un comportamento normale e il rilevamento di anomalie rendono possibile il rilevamento degli abusi delle API, che spesso non possono essere rilevati attraverso schemi o firme. Inoltre, la possibilità di ripercorrere l'attacco e vedere ciò che è accaduto prima di un avviso fornisce preziose informazioni sull'uso e l'abuso del patrimonio delle API.

Funzionalità critica n. 8
Risposte personalizzate e automatizzate

I sistemi online tradizionali possono eseguire azioni automatizzate per bloccare sospetti attacchi alle API, purché le organizzazioni siano in grado di identificarli tempestivamente. Poiché l'analisi comportamentale e il rilevamento delle anomalie vengono eseguiti nel lungo periodo e con un contesto aziendale molto più ampio, la profondità del rilevamento consente di far emergere le anomalie. In questo modo viene abilitata un'ampia gamma di risposte automatizzate e personalizzate, che possono essere eseguite con elevata precisione. Alcuni esempi sono:

- Blocco o limitazione del traffico nei gateway delle API supportati e filtri sull'edge CDN
- Notifiche e-mail per gli esperti della sicurezza e dell'azienda
- Creazione di ticket per gli sviluppatori
- Attivazione di webhook

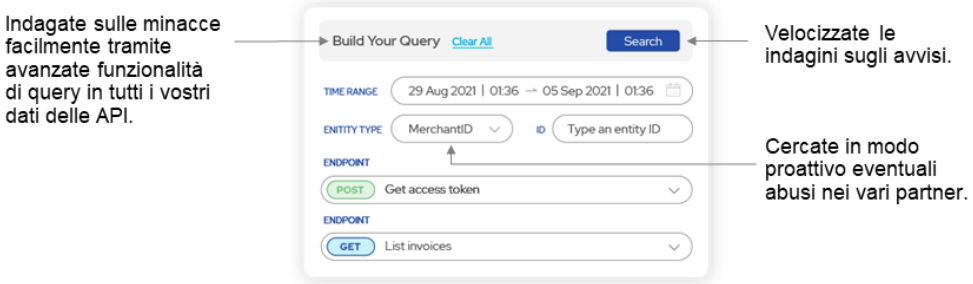
Risposte personalizzabili in base ai processi aziendali



Funzionalità critica n. 9
Indagine proattiva e ricerca delle minacce

Molte organizzazioni non possono concedersi il lusso di aspettare che si verifichi un incidente di sicurezza prima di agire. Un approccio più efficace consiste nell'identificare situazioni indesiderate e ricercarle attivamente. Ad esempio, un avviso che ha rilevato un abuso a un'API può essere utilizzato adottando lo stesso comportamento su un'altra API tramite la ricerca proattiva delle minacce. Di conseguenza, oltre agli avvisi generati in risposta agli incidenti attivi, una piattaforma di protezione dalle minacce alle API deve poter ricercare comportamenti specifici. Le funzionalità di ricerca delle minacce richiedono l'accesso ai dati cronologici per poter individuare una violazione nascosta delle API. Le soluzioni a singola richiesta, che non arricchiscono i dati e non forniscono un contesto, non sono idonei a definire attività coerenti. La ricerca delle minacce e le indagini si basano sui dati cronologici.

Il potere di indagare e ricercare le minacce a portata di mano



Funzionalità critica n. 10
Data lake osservabile

Tra tutte le funzionalità necessarie per una solida strategia di sicurezza, il contesto è fondamentale per proteggere qualsiasi API nel lungo periodo. Il modo migliore per creare un contesto in grado di segnalare le minacce, identificare potenziali vulnerabilità e risolvere i problemi in caso di attacco consiste nel registrare tutti i comportamenti delle API e mantenere un backlog di questa attività. Per farlo, è possibile associare un data lake alla soluzione di sicurezza delle API. Cercate un data lake che fornisca la maggiore quantità di dettagli cronologici al fine di sviluppare la vostra strategia. Sebbene l'inserimento dei dati nei modelli di apprendimento automatico possa essere utile, avere dettagli come i parametri della richiesta consente alle organizzazioni di agire efficacemente sui loro dati cronologici per proteggerli da minacce e attacchi futuri.

N. 1 - Protezione indipendente dalla piattaforma	L'ampia visibilità della piattaforma proteggerà la vostra organizzazione dalle minacce interne e dagli abusi.
N. 2 - Rilevamento continuo delle API e gestione del sistema	Un inventario completo e sempre aggiornato di tutte le API in uso nell'organizzazione è alla base di ogni strategia vincente, perché le organizzazioni non sono in grado di proteggere elementi che non sanno di avere nel loro ambiente.
N. 3 - Visualizzazione del comportamento delle API	La visibilità è necessaria per consentire agli esperti della sicurezza, dello sviluppo e delle operazioni di visualizzare e comprendere le modalità di utilizzo o abuso delle API, affinché possano garantire la comunicazione tra team e analizzare i vari casi.
N. 4 - Tracciamento di più entità utente	Comprendere l'entità ed essere in grado di vedere le attività delle API correlate fornisce un contesto utile per identificare possibili usi o abusi, pertanto è fondamentale che la piattaforma di protezione abbia la capacità di monitorare singolarmente ciascuna entità.
N. 5 - Copertura B2B (da azienda ad azienda) e API est-ovest	Per fornire un quadro completo delle attività delle API e dell'esteso panorama delle minacce, le organizzazioni devono adottare un approccio che assicuri visibilità, osservabilità e monitoraggio, efficaci per tutti i casi di utilizzo.
N. 6 - Analisi comportamentale e rilevamento	Per sapere se il comportamento di un'API è anomalo, evento che indica che potrebbe essere compromessa, è necessario analizzare il suo impiego sul lungo periodo. La tecnica dell'analisi comportamentale identifica uno standard normale e monitora costantemente il comportamento per rilevare eventuali anomalie.
N. 7 - Avvisi significativi con contesto	Quando un'organizzazione ha visibilità su tutte le attività delle API e le analisi comportamentali, gli avvisi acquisiscono maggiore significato. Le organizzazioni possono eliminare la necessità di anticipare ogni possibile attacco, rendendo più astratto l'approccio al monitoraggio della sicurezza.

N. 8 - Risposte personalizzate e automatizzate	Poiché l'analisi comportamentale e il rilevamento delle anomalie vengono eseguiti nel lungo periodo e con un contesto aziendale molto più ampio, la profondità del rilevamento consente di far emergere le anomalie. In questo modo viene abilitata un'ampia gamma di risposte automatizzate e personalizzate, che possono essere eseguite con elevata precisione.
N. 9 - Indagine proattiva e ricerca delle minacce	Molte organizzazioni non possono concedersi il lusso di aspettare che si verifichi un incidente di sicurezza prima di agire. Un approccio più efficace consiste nell'identificare situazioni indesiderate e ricercarle attivamente.
N. 10 - Data lake osservabile	Il modo migliore per creare un contesto in grado di segnalare le minacce, identificare potenziali vulnerabilità e risolvere i problemi in caso di attacco consiste nel registrare tutti i comportamenti delle API e mantenere un backlog di questa attività. Per farlo, è possibile associare un data lake alla piattaforma di sicurezza delle API.

Se pensate che questo testo sia stato utile, il passo successivo sarà quello di scoprire la soluzione Akamai API Security per implementare la strategia di sicurezza delle API più efficace possibile.

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com e akamai.com/blog, oppure seguite Akamai Technologies su X, in precedenza Twitter, e su LinkedIn. Data di pubblicazione: 12/23.