Akamai

WHITE PAPER

11 funzionalità critiche di rilevamento e risposta alle minacce delle API

L'evoluzione della strategia di sicurezza delle API

Introduzione

Le API svolgono un ruolo fondamentale in ogni applicazione che la vostra organizzazione crea per i suoi clienti, utilizza internamente e rende disponibile per vendor e fornitori. Cosa fanno le API? Scambiano informazioni (spesso dati sensibili) tra uno strumento tecnologico e l'altro. E dove si trovano le API? Non solo nelle applicazioni, ma anche nelle implementazioni migrate sul cloud, negli strumenti dell'AI generativa e nella supply chain digitale.

La loro sfida: le API rappresentano anche una parte significativa nella superficie di attacco della vostra organizzazione.

Nella corsa all'innovazione delle aziende, le API vengono spesso sviluppate frettolosamente, sottoposte a test inadeguati e rilasciate in fase di produzione con errori di configurazione e controlli di sicurezza mancanti. Inoltre, le API sono proliferate al punto che i team addetti alla sicurezza non dispongono della visibilità necessaria su gran parte delle loro API. Senza un'appropriata visibilità, le organizzazioni:

1. Non è possibile rilevare le API non gestite, dimenticate e rese visibili per i loro dati sensibili, su Internet e ai criminali
2. D'altro canto, non è possibile valutare i rischi per le API, ad esempio, solo il 27% (una percentuale in calo dal 40% registrato nel 2023) delle aziende con un inventario completo delle API sa quali delle loro API restituiscono dati sensibili
3. Alla fine, potreste ritrovarvi con una superficie di attacco piena di vulnerabilità legate alle API che i criminali sfruttano frequentemente (e, spesso, facilmente)

Si sono basate finora su una serie di strumenti comunemente usati per gestire le API e ottenere un certo livello di protezione. Tuttavia, se l'84% delle organizzazioni ha riscontrato un problema di sicurezza delle API negli ultimi 12 mesi, con un aumento rispetto al 78% registrato nel 2023, qualcosa deve cambiare.

Poiché gli attacchi alle API crescono in numero e complessità, è il momento di considerare la possibilità di aggiungere nuovi livelli di protezione ad alcuni strumenti, come gateway API, soluzioni WAF (Web Application Firewall) e piattaforme WAAP (Web Application and API Protection).

Questi nuovi livelli aumentano la visibilità su tutte le API presenti nel vostro ambiente e sui loro rischi, inclusa la gran parte delle API non gestite, come:

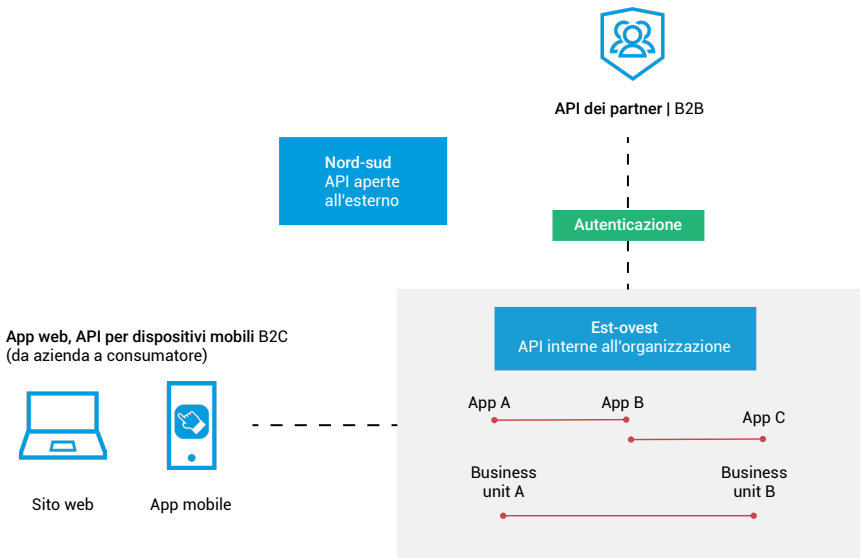
- API zombie che dovrebbero essere dismesse, ma rimangono attive
- API ombra non documentate che dovrebbero essere eliminate o spostate in processi di governance formali.

Le organizzazioni devono disporre di funzionalità approfondite per rilevare e mitigare gli abusi e gli attacchi alle API, incluse le minacce riportate nell'elenco OWASP con i 10 principali rischi per la sicurezza delle API. Inoltre, con un'attenzione particolare rivolta all'individuazione e alla mitigazione delle vulnerabilità nell'ambito di un ciclo di vita completo delle API, le aziende devono adottare un rigoroso processo di esecuzione dei test sulla sicurezza delle API in tempo reale, dalle fasi iniziali dello sviluppo fino alla produzione.

Ciò significa aggiungere un nuovo strumento per ogni problema riscontrato? No, al contrario, si tratta più di garantire l'utilizzo degli strumenti appropriati per il compito da svolgere, come in un'orchestra per poter suonare le giuste note al momento giusto e con una coordinazione precisa con le relative controparti.

Se pensate a come aggiungere nuovi livelli di protezione delle API, considerate l'approccio basato su una difesa approfondita che viene applicato dai team addetti alla sicurezza ad altre minacce, ad esempio, l'implementazione di una serie di controlli per rilevare, prevenire e mitigare gli effetti di un attacco ransomware. È proprio così che le organizzazioni devono considerare le API.

In questo white paper, verranno esaminate 11 funzionalità critiche che potete integrare nella vostra strategia per la sicurezza delle API incentrata sul rilevamento e sulla risposta alle minacce delle API.



Il contesto è la chiave

In che modo le attività di rilevamento e risposta alle minacce delle API si inseriscono nella relativa strategia di protezione?

Come forse avrete visto direttamente, le API hanno cambiato il modo di operare delle aziende perché assicurano un maggior numero di casi di utilizzo, accelerano i cambiamenti, includono più dati sensibili e sono aperte a più utenti. Non sorprende che le organizzazioni abbiano creato molti più canali delle API che interfacce per applicazioni web. Inoltre, i rischi risultano amplificati perché le API sono integrate con un numero sempre maggiore di logica e dati aziendali importanti.

Considerando la prevalenza delle API nella miriade di tecnologie che vengono già protette dai team addetti alla sicurezza (ossia, le applicazioni), la maggior parte delle categoria di prodotti per la sicurezza supporta in qualche modo le API. Tuttavia, API e applicazioni non sono uguali, ma vengono persino considerate come risorse diverse in alcuni quadri di conformità. Non è sufficiente aggiungere funzionalità frammentarie per la protezione dalle minacce alle API, ad esempio, ad un prodotto esistente per la sicurezza delle applicazioni. Le API meritano una maggiore attenzione rispetto a quella che, solitamente, ricevono nella maggior parte delle organizzazioni. Oggi, i team addetti alla sicurezza devono considerare le API come una classe di risorse separata con una serie distinta di attributi di rischio e cercare le funzionalità critiche in grado di proteggerle totalmente e su vasta scala.

In passato, se un'organizzazione disponeva di un inventario delle API e di alcuni strumenti basilari per la gestione e la protezione delle API, aveva buone possibilità di prevenire i più comuni attacchi alle API. Sfortunatamente, oggi i criminali spesso sono più sofisticati come le aziende, con un'attenzione simile al miglioramento continuo.

- I criminali, logicamente, stanno evolvendo le loro tattiche per eludere gli strumenti a loro noti su cui la maggior parte delle organizzazioni si basa per difendere le proprie API.
- Analogamente al modo con cui la maggior parte delle aziende utilizza l'AI, i criminali stanno aumentando le loro limitate capacità umane con un'assistenza continua offerta dalle funzionalità dell'AI generativa.
- I criminali cercano sempre più gli anelli deboli della supply chain digitale delle API aziendali, come i partner B2B di un'azienda che potrebbero non dare priorità alla protezione delle API.

Ad esempio, alcune forme di abuso delle API provengono da clienti e partner ai quali sono state concesse le credenziali delle API, che, tuttavia, utilizzano in modo non autorizzato. Esistono anche metodi per dirottare le credenziali o i token di sicurezza delle API apparentemente legittimi. Le vulnerabilità nascoste nelle implementazioni dei client delle API sono un altro vettore di attacco che i criminali 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 dai metodi di attacco in rapida evoluzione sono disponibili per le organizzazioni. Scoprite ulteriori informazioni sulle 11 funzionalità principali con cui il vostro team può iniziare mentre vi occupate della protezione delle API (e dei dati che trasmettono) dagli attacchi.

Funzionalità critica n. 1

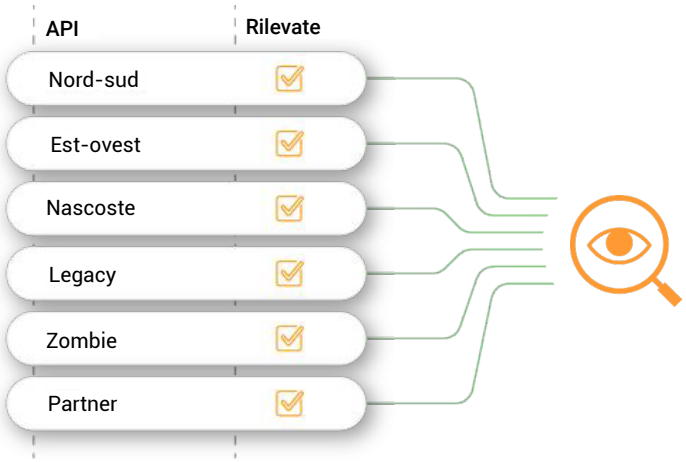
Individuazione continua e gestione del sistema di sicurezza delle API

Un inventario completo e sempre aggiornato delle 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 componenti che non sa di avere nel suo ambiente. Molte aziende di prodotti per la sicurezza affermano di poter individuare le API in modo efficace, 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:

- L'individuazione automatica e continua delle API, 24 ore su 24, inclusa l'individuazione delle API utilizzate una sola volta (l'individuazione on-demand o giorno per giorno non è sufficiente)
- L'individuazione delle API nelle diverse tecnologie e infrastrutture in uso
- L'individuazione delle API appena distribuite e il confronto con le API ben documentate per identificare le API ombra
- La valutazione del rischio per ogni endpoint e servizio delle API aiuta i team addetti alla sicurezza e allo sviluppo a capire le reali capacità e a dare priorità alle API con il massimo impatto potenziale, se violate
- Il rilevamento delle istanze delle vulnerabilità note delle API, come quelle riportate nell'elenco OWASP con i 10 principali rischi per la sicurezza delle API

Migliore visibilità

Non perdete più di vista l'inventario delle vostre API



Funzionalità critica n. 2
Visibilità sul comportamento delle API

La visibilità sul comportamento effettivo delle API (chiamate API) rappresenta una funzionalità fondamentale per una piattaforma di sicurezza delle API. Questa funzionalità è necessaria per consentire ai team addetti alla sicurezza, allo sviluppo e alle operazioni di visualizzare e comprendere le modalità di utilizzo o abuso delle API, affinché possano garantire la comunicazione tra i team e analizzare i vari casi. Alcune delle funzionalità che consentono la visibilità 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.
- **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. Una soluzione deve analizzare il traffico e inviare solo i metadati pertinenti per aggiornare i dashboard.

Funzionalità critica n. 3

Rilevamento dei tentativi di abuso delle API tramite le informazioni sulle entità utente

I team addetti alla sicurezza hanno bisogno della capacità di monitorare le attività dannose contro entità specifiche, come indirizzi IP, e processi aziendali, come ID di pagamento. Questa capacità può risultare preziosa se combinata con funzionalità in grado di correlare gli attacchi provenienti da diversi IP in istanze quando altri identificatori rilevanti possono offrire informazioni sull'abuso delle API.

Prendiamo, ad esempio, un utente sconosciuto che effettua una chiamata all'API di un'azienda di retail utilizzando /api/getpaymentID/50 come identificativo. In questo caso, il team addetto alla sicurezza del retailer sa che tutti gli altri utenti della piattaforma dell'azienda sono legati ad un solo tipo di ID di pagamento. Se un analista della sicurezza si accorge improvvisamente che l'utente sconosciuto sta effettuando chiamate ripetute, ogni volta modificando leggermente il numero ID (/api/getPaymentID/51 … 52 … 53 … 54), si tratta di un importante indicatore di un tentativo di abuso delle API.

Acquisire informazioni in tempo reale sui comportamenti atipici degli utenti può fare la differenza tra un tentativo di attacco contrastato e un attacco alle API riuscito.

943.162 dollari

Costo medio necessario per rimediare agli incidenti di sicurezza delle API, secondo i CISO, i CIO e i CTO che hanno riferito di aver subito eventi di questo tipo negli ultimi 12 mesi.

Per ulteriori informazioni sulle opinioni e sulle esperienze dei vostri colleghi, potete consultare lo studio sull'impatto della sicurezza delle API nel 2024.

Funzionalità critica n. 4
Analisi e rilevamento delle anomalie dei comportamenti

Anche se l'analisi delle singole chiamate API da parte degli utenti, o persino delle singole sessioni, può aiutare i team addetti alla sicurezza, è importante riuscire a rilevare le minacce alle API in modo completo per avere un quadro generale. Cercate le funzionalità necessarie per poter comprendere in modo approfondito i modelli e le anomalie dei comportamenti nell'intero patrimonio delle API. Per stabilire se il comportamento di un'API è anomalo, a indicare che potrebbe essersi verificata una violazione, è necessario analizzare il suo utilizzo per lunghi periodi di tempo con un contesto generato dal monitoraggio del comportamento. In tal modo, i team addetti alla sicurezza possono disporre di uno standard affidabile monitorando costantemente il comportamento per rilevare eventuali anomalie.

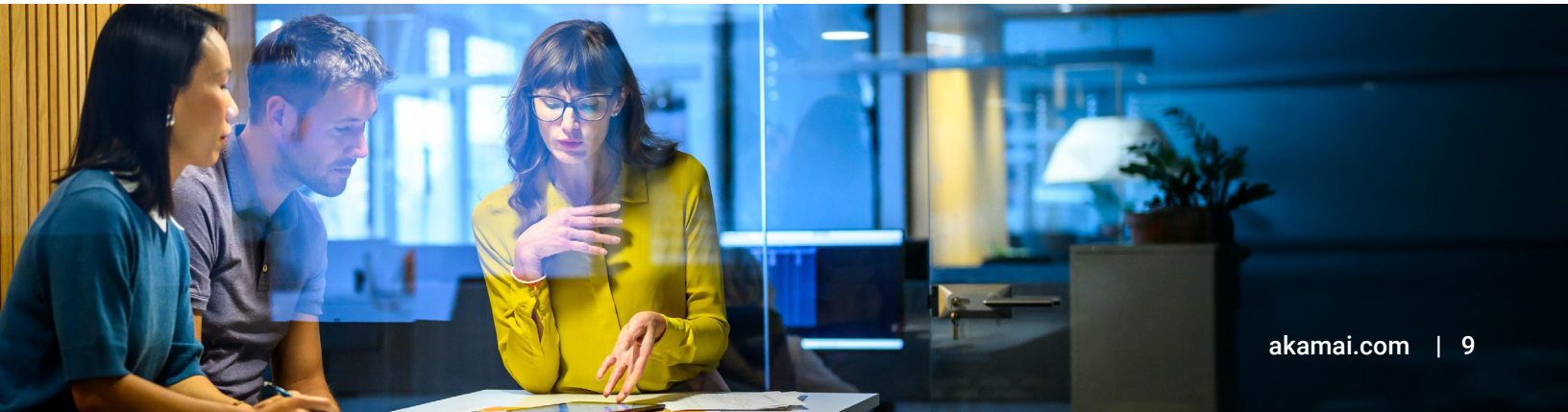
Funzionalità critica n. 5
Rilevamento delle deviazioni nelle specifiche delle API

Le API fluiscono costantemente nell'ambito della domanda del mercato e nei requisiti aziendali in continua evoluzione. Di conseguenza, le organizzazioni stanno rilasciando continuamente nuove implementazioni di endpoint allo scopo di soddisfare le esigenze aziendali in rapida evoluzione. L'aggiornamento della documentazione delle API per riflettere queste cambiamenti sulla base delle specifiche delle API è fondamentale e, soprattutto, bisogna prestare particolare attenzione a garantire che il traffico delle API sia sempre allineato alle relative specifiche.

Per rendere le API resilienti agli abusi e agli attacchi, le organizzazioni devono cercare funzionalità in grado di rilevare le deviazioni nelle specifiche delle API. In tal modo, le aziende possono individuare eventuali discordanze o lacune nella documentazione delle API confrontando continuamente il traffico delle API in tempo reale con le specifiche definite.

Se la funzione di rilevamento delle deviazioni nelle specifiche delle API individua mancate corrispondenze o endpoint non documentati a cui si è tentato di accedere in fase di produzione, vengono inviati appositi avvisi agli sviluppatori e ai team addetti alla sicurezza, che, in tal modo, possono:

- Stare al passo con i problemi prima che possano peggiorare
- Garantire che le API funzionino nel modo previsto
- Rafforzare la sicurezza delle applicazioni supportate dalle API
- Mantenere l'integrità dell'ecosistema delle API aziendali



Funzionalità critica n. 6
Copertura delle API est-ovest e B2B (da azienda ad azienda)

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

Benché le applicazioni web B2C (da azienda a consumatore) beneficino della protezione offerta 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 anche passando attraverso le soluzioni WAAP.

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. 7
Avvisi significativi con contesto

Quando un'organizzazione ha visibilità sulle attività delle sue API e sulle analisi comportamentali su larga scala, gli avvisi sulle loro attività acquisiscono maggiore significato. Tuttavia, come potete assicurarvi di rivolgere la massima attenzione e tutte le risorse possibili nella lotta contro le reali minacce alle API? Un motore di valutazione dell'affidabilità dei criminali può utilizzare gli algoritmi di apprendimento automatico per valutare i segnali interni ed esterni, tra cui il comportamento delle API, i modelli del traffico di rete, i dati di geolocalizzazione, i feed di intelligence sulle minacce e altri fattori contestuali, per stabilire il livello di affidabilità secondo cui un incidente di runtime rilevato sia il risultato di un'attività dannosa. Questa funzionalità può aiutare i team addetti alla sicurezza ad eliminare le minacce critiche e deve essere combinata con funzioni in grado di creare flussi automatici di mitigazione e notifica per gli attacchi ad alto impatto.

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 API e nei filtri sull'edge per le reti per la distribuzione dei contenuti (CDN) supportati
- Notifiche e-mail per gli addetti alla sicurezza e le parti interessate dell'azienda
- Creazione di ticket per gli sviluppatori
- Attivazione di webhook

Cosa possono fare le organizzazioni per aiutare i team addetti alla sicurezza già sotto pressione per massimizzare i loro team e le loro energie nel momento in cui si assiste ad un aumento delle minacce alle API? Cercate funzionalità di automazione in grado di migliorare l'efficienza e la produttività semplificando la creazione e la gestione di workflow multiazione. Le giuste funzionalità di automazione devono offrire un'interfaccia di sviluppo visiva senza codice in grado di creare complessi processi di risposta agli eventi e di sincronizzare i dati relativi agli incidenti tra le principali soluzioni per la sicurezza delle API e una miriade di servizi di terze parti, tra cui ServiceNow, Jira e Azure DevOps.

Funzionalità critica n. 9
Analisi del traffico delle API

Le organizzazioni hanno bisogno di funzionalità always-on per la registrazione, la visibilità e l'analisi del traffico delle API nei loro ambienti senza implementare un data lake. Registrando i flussi dei dati delle API che corrispondono a specifici criteri negli ambienti delle applicazioni, incluse le attività delle API tipiche e quelle anomale, le organizzazioni possono cercare le minacce in modo più efficace, gestendo, nel contempo, il rischio di riscontrare utenti sospetti e comportamenti delle API insoliti. È importante disporre di funzioni di audit del traffico delle API in grado di adattarsi specificamente a particolari casi di utilizzo per consentire alle organizzazioni di acquisire e mantenere il traffico secondo regole e filtri prestabiliti.

Funzionalità critica n. 10
Test delle API rigorosi e in tempo reale

Nella corsa all'innovazione, le organizzazioni stanno rilasciando le API in fase di produzione con vulnerabilità e difetti di progettazione spesso non rilevati. Le organizzazioni possono prevenire questi problemi adottando un approccio Shift-Left all'esecuzione dei test delle API in fase di sviluppo. Tra le funzionalità principali, figurano le seguenti:

- Esecuzione di test automatizzati in grado di simulare il traffico dannoso, inclusi i tipi riportati nell'elenco OWASP con i 10 principali rischi per la sicurezza delle API
- Verifica delle specifiche delle API sulla base delle regole e delle policy di governance stabilite
- Esecuzione di test sulle API on-demand o come parte di una pipeline CI/CD

Funzionalità critica n. 11
Protezione indipendente dalla piattaforma

Generalmente, i servizi delle API sono implementati da diversi gruppi all'interno di un'organizzazione, che spesso utilizzano molteplici piattaforme e tecnologie. Alcune API vengono, ad esempio, implementate on-premise, mentre altre sono eseguite nel cloud pubblico. Spesso, le organizzazioni utilizzano tecnologie intermedie, quali proxy inversi, gateway API, WAF e CDN, che offrono vantaggi commerciali, ma ostacolano la visibilità sulle API.

La capacità di accedere ai dati sulle attività delle API da ciascuna di queste tecnologie è fondamentale. Un approccio di protezione delle API indipendente dalla piattaforma garantisce alla vostra organizzazione un quadro sempre completo delle 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

Un approccio indipendente dalla piattaforma estende anche la visibilità oltre le API nord-sud, includendo, inoltre, 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.

Conclusione

Le API sono componenti essenziali per consentire ad un'organizzazione di offrire servizi ai clienti, generare profitti e operare in modo efficiente nell'economia dei nostri giorni sempre più digitale e incentrata sul cloud. Tuttavia, la crescita continua, la vicinanza ai dati sensibili e la mancanza di controlli di sicurezza delle API le rendono una notevole fonte di rischio.

Akamai API Security fornisce tutte le 11 funzionalità critiche descritte in questo white paper, aiutando le organizzazioni a basarsi sul loro approccio esistente con funzioni essenziali, come:

- Individuazione delle API
- Valutazione dei rischi (inclusa l'esposizione dei dati sensibili)
- Rilevamento degli abusi e degli attacchi alle API
- Esecuzione di test sulle API per rilevare vulnerabilità e rischi per la sicurezza

Scoprite ulteriori informazioni sulla protezione dai 10 principali rischi alla sicurezza delle API identificati dall'OWASP.

Scoprite come possiamo aiutarvi programmando una demo personalizzata su Akamai API Security.

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 modo che 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 e akamai.com/blog o seguite Akamai Technologies su X, in precedenza Twitter, e LinkedIn. Data di pubblicazione: 01/25.