IDC MarketScape

IDC MarketScape: valutazione dei produttori delle piattaforme aziendali di protezione delle applicazioni Web e delle API a livello globale per il 2024

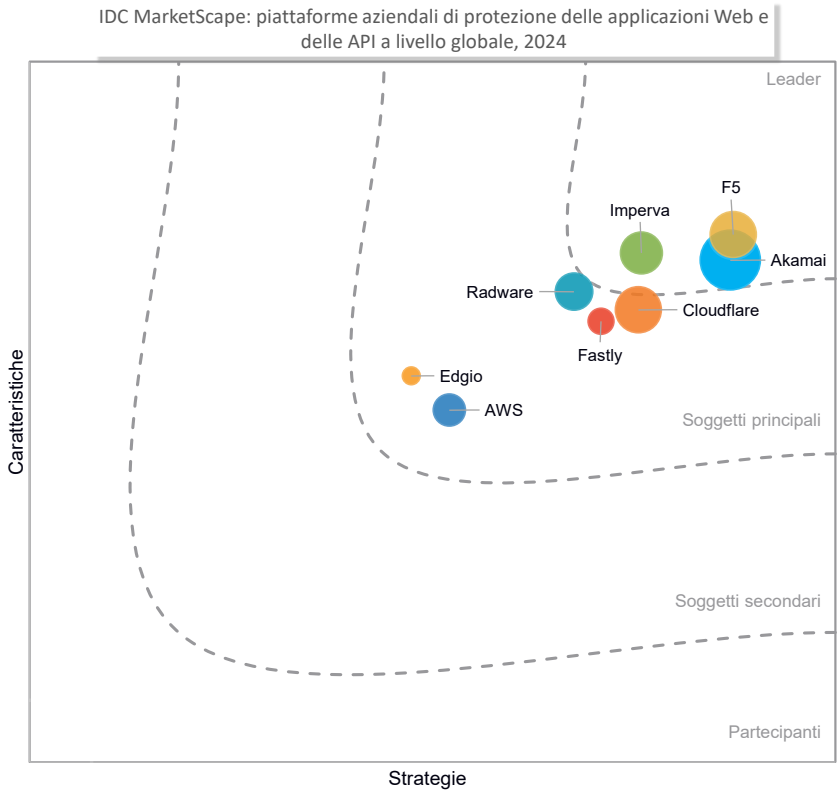
Christopher Rodriguez

QUESTO ESTRATTO DI IDC MARKETSCAPE VERTE SU AKAMAI

FIGURA DI IDC MARKETSCAPE

FIGURA 1

IDC MarketScape: valutazione dei produttori delle piattaforme aziendali di protezione delle applicazioni Web e delle API a livello globale



Fonte. IDC, 2024

September 2024, IDC US51795524e

Consultare l'appendice per la metodologia dettagliata, la definizione del mercato e i criteri di assegnazione dei punteggi.

IN QUESTO ESTRATTO

Il contenuto del presente documento è tratto dal testo "IDC MarketScape: Worldwide Web Application and API Protection Enterprise Platforms 2024 Vendor Assessment (doc n. US51795524). Tutte le seguenti sezioni (o parte di esse) sono state inserite nel presente estratto: "L'opinione di IDC", "Criteri di inclusione dei produttori di IDC MarketScape", "Guida di base", "Profilo riepilogativo dei produttori", "Appendice" e "Ulteriori informazioni". Sono incluse anche le figure 1 e 2.

L'OPINIONE DI IDC

Le applicazioni Web sono componenti fondamentali delle moderne aziende digitali. Esse offrono le funzionalità necessarie per interagire con i clienti acquisiti e potenziali, partner, ospiti, dipendenti e collaboratori. I criminali informatici analizzano queste applicazioni e le relative interfacce di programmazione (application programming interface, API) per appropriarsi dei dati, ottenere un accesso illecito o danneggiare le aziende per conseguire guadagni personali criminosi. Gli attacchi rivolti alle applicazioni Web e alle API hanno causato violazioni di alto profilo, costosi tempi di inattività e furti. Gli utenti finali e i clienti subiscono spesso il peso di questo fenomeno attraverso perdite finanziarie in grado di compromettere la loro fiducia e spingerli a ridurre gli affari online.

Il crimine informatico online è un fenomeno molto grave che può danneggiare gravemente i risultati aziendali. Nel corso degli anni, le aziende hanno adottato numerosi strumenti di sicurezza per contrastare le nuove tattiche di attacco e l'espansione delle superfici d’azione dei criminali. Un Web Application Firewall (WAF) è una tecnologia che offre una protezione di base nei confronti degli attacchi noti ed emergenti a livello applicativo. Le aziende hanno implementato anche svariate soluzioni specializzate, come ad esempio mitigazione dei DDoS, gestione dei bot e, più recentemente, sicurezza delle API.

La protezione delle applicazioni Web e delle API (Web Application and API Protection, WAAP) unisce le tecnologie di sicurezza di base in una piattaforma integrata, coerente e che offre un livello affidabile di protezione dalle minacce online. Le piattaforme consolidate e integrate consentono di ridurre le lacune in termini di sicurezza e complessità di gestione, semplificando le ispezioni. Secondo una ricerca di IDC, il 77% delle aziende considera l'integrazione tra le soluzioni di sicurezza come un elemento

"importante" o "di valenza critica". Le applicazioni subiscono numerosi attacchi ogni giorno. I criminali sfruttano diverse tattiche per individuare i punti deboli delle difese. Di conseguenza, le strategie di sicurezza delle applicazioni basate su una protezione isolata e specializzata sono destinate al fallimento. La convergenza e il consolidamento della sicurezza sono un elemento fondamentale per ottenere una protezione più efficace, sia attraverso una maggiore precisione del rilevamento che mediante la riduzione dei falsi positivi e l'individuazione affidabile delle minacce avanzate e zero-day.

In ogni modo, la convergenza offre anche vantaggi di business, come ad esempio la riduzione dei tempi e delle risorse di implementazione e gestione, il miglioramento dell'esperienza utente e l'ottimizzazione delle analisi. Inoltre, l'esecuzione di tutte le funzionalità di sicurezza attraverso un singolo servizio riduce la latenza legata all'instradamento del traffico verso diversi punti in cui eseguire le ispezioni di sicurezza.

Allo stesso tempo, le aziende devono adottare un approccio misurato, implementando le tecnologie di protezione delle applicazioni in modo graduale, in base alle necessità o al tempo e alle risorse disponibili. I clienti richiedono una piattaforma modulare e integrata che consenta di implementare la WAAP in modo semplice con il tempo. I produttori devono individuare l'esatta combinazione delle caratteristiche integrate nelle aree funzionali di base della sicurezza da includere nei diversi livelli del prodotto.

Anche se il WAF è un componente fondamentale, non è possibile proteggere le applicazioni moderne senza una strategia coerente relativa alle API, che ricoprono un ruolo essenziale nella moderna era del business digitale. Occorre un processo semplificato ed efficiente per l'integrazione delle applicazioni e l'offerta di nuove e potenti funzionalità. Tuttavia, le API modificano la superficie di attacco in modi sempre diversi, sono vulnerabili alle configurazioni errate, all'esposizione di dati sensibili, agli attacchi denial-of-service e a molti altri che colpiscono le interfacce utente, ma sono soggette a minacce specifiche come ad esempio la broken object-level authorization (BOLA). Le API gestiscono anche la comunicazione fra le applicazioni, che potrebbero essere bloccate da una soluzione di protezione perimetrale come il WAF, causando falle di sicurezza che i criminali potrebbero sfruttare per spostarsi lateralmente dietro le difese di rete.

La combinazione di WAF e sicurezza delle API offre una copertura completa delle applicazioni Web su tutte le interfacce e superfici di attacco. La proposta a valore della WAAP si basa sulle tecnologie in grado di gestire minacce specifiche come ad esempio gli attacchi DDoS e le attività indesiderate dei bot. Queste minacce variano notevolmente in termini di facilità di rilevamento, difficoltà di mitigazione, frequenza dell'occorrenza e gravità dell'impatto. In definitiva, uno stack completo di protezione delle applicazioni richiede la sicurezza WAF e delle API, la mitigazione de DDoS e la

gestione dei bot. I requisiti tecnici delle API e le esigenze specifiche degli attacchi DDoS e delle attività dei bot rendono lungo e tortuoso il passaggio alle soluzioni WAAP.

CRITERI PER L'INCLUSIONE DEI PRODUTTORI IN IDC MARKETSCAPE

La WAAP è una soluzione di sicurezza convergente per la protezione attiva delle applicazioni incentrata sul WAF. IDC ha identificato le caratteristiche principali, analizzate in questa sezione, per l'inserimento di questo tipo di soluzioni nell'analisi MarketScape per le piattaforme aziendali WAAP.

I produttori devono offrire una soluzione WAAP convergente che unisca almeno due dei seguenti elementi in una singola piattaforma di sicurezza:

- Sicurezza delle API
- Gestione dei bot
- Mitigazione del DDoS
- Firewall per le applicazioni Web

Il WAF è un elemento fondamentale per ogni soluzione WAAP. Inoltre, le vendite una tantum dei componenti WAAP come soluzioni autonome non verranno conteggiate come un prodotto WAAP completo.

Questa analisi di IDC MarketScape si basa sui seguenti requisiti per la partecipazione e presenza sul mercato:

- **Partecipazione sul mercato.** Un produttore deve offrire caratteristiche WAAP critiche come soluzione unificata a partire dal 2023. È possibile fornire specifiche funzionalità di base o estese nell'ambito di un altro bundle o una piattaforma, o come soluzioni autonome, a patto che non vengano offerte solo come prodotti autonomi o separati. Per una descrizione completa e dettagliata delle caratteristiche necessarie e opzionali, consultare la sezione "Definizione del mercato".
- **Rappresentazione del mercato.** Un produttore deve aver raggiunto una quota minima di fatturato nel mercato competitivo WAAP nel 2023, come confermato dal Security Products Tracker di IDC.
- **Presenza globale.** Un produttore deve ottenere il proprio fatturato in ciascuna delle principali regioni globali, tra cui Nord America, America Latina, EMEA e Asia/Pacifico, a partire dal 2024 e secondo quanto confermato dal Security Products Tracker di IDC.

Alcuni produttori di soluzioni cloud e di sicurezza che offrono solo qualche componente di un prodotto WAAP non sono stati inclusi nell'analisi, in quanto offrono una soluzione specifica e non un approccio WAAP integrato. Allo stesso modo, alcuni produttori di

soluzioni WAAP non hanno soddisfatto i requisiti minimi di rappresentanza del mercato o presenza globale.

SUGGERIMENTO PER GLI ACQUIRENTI DELLE TECNOLOGIE

Considerazioni di base sulle capacità dei produttori

L'analisi di IDC MarketScape sulle piattaforme aziendali WAAP tiene conto del livello comune di protezione richiesto e previsto dagli acquirenti IT, oltre al grado di integrazione, della facilità d'uso, dei servizi professionali e gestiti adiacenti e al costo totale di proprietà. A livello aziendale, una WAAP deve offrire una protezione eccellente, ridurre l'impatto della sicurezza sulle prestazioni e causare pochissimi conflitti in termini di esperienza dell'utente finale. L'analisi sottolinea anche l'obiettivo principale delle WAAP, ovvero l'unione di diverse tecnologie di sicurezza di base in una singola piattaforma integrata e coerente. Inoltre, le soluzioni devono essere espandibili e dotate di diversi modelli di prezzo. Ciò consente alle WAAP di offrire una protezione coerente nei confronti delle numerose minacce online e un considerevole valore aziendale.

Le aspettative degli utenti continuano a crescere. Le aziende continuano ad adottare tecnologie emergenti per offrire esperienze utente innovative e scorrevoli. Le applicazioni fanno sempre più affidamento su infrastrutture complesse e distribuite. I team DevOps lavorano in modo più rapido e intelligente per lanciare le nuove funzionalità sul mercato. Le aziende intendono valutare le caratteristiche specifiche del prodotto e delle funzioni offerte (o non offerte) dai produttori in modo nativo. Si tratta di elementi inseriti nella soluzione per impostazione predefinita o attraverso altri mezzi, come ad esempio le caratteristiche aggiuntive di prime parti, i prodotti separati, le funzionalità degli OEM di terze parti o le integrazioni tecniche. È possibile anche effettuare ulteriori considerazioni.

- **WAF lato client.** Il WAF lato client, detto anche "protezione lato client", è una tecnologia di sicurezza emergente che contrasta un vettore di minacce specifico: il codice delle applicazioni Web che viene eseguito sui dispositivi degli utenti finali. Questo codice comprende gli script eseguiti nel browser, e non su un server Web, per svolgere diverse funzioni sul dispositivo.
- **Prevenzione delle frodi e degli usi impropri.** Di solito, le funzionalità di prevenzione delle frodi e degli usi impropri online si basano in genere su capacità di gestione dei bot, specificamente studiate per affrontare i modelli univoci indicativi di specifiche attività fraudolente,, come ad esempio l'appropriazione indebita di un account o la frode di nuovi account (detta anche frode degli account falsi). Per rilevare in modo completo frodi e altre azioni che indicano un abuso di applicazioni e API correttamente funzionanti, occorre

eseguire approfondimenti sull'identità degli utenti, sulla telemetria a livello di client e dispositivo e sul comportamento dell'utente. Di conseguenza, esistono differenze significative tra le soluzioni WAAP in termini di capacità di rilevamento delle frodi e modalità di fornitura di queste funzionalità agli acquirenti.

- **Proxy residenziali.** Le soluzioni WAAP agiscono in modo diverso nel rilevamento dei criminali nascosti dietro proxy residenziali o che si avvalgono di altri metodi di offuscamento come ad esempio la rotazione degli IP.
- **WebSockets.** Supporto delle applicazioni che utilizzano WebSockets, un protocollo che offre comunicazioni in tempo reale con una connessione full duplex. Il supporto per WebSockets è sempre più importante, poiché gli utenti intendono utilizzare applicazioni interattive e in tempo reale.
- **WebAssembly (WASM).** Linguaggio di basso livello che fornisce un formato di codice binario portabile. Il vantaggio principale di WASM è la capacità di supportare facilmente un'ampia gamma di linguaggi di sviluppo. L'importanza del supporto di WASM nelle soluzioni WAAP aumenta insieme alla portata dell'adozione.
- **Autoprotezione delle applicazioni in tempo reale (RASP).** La RASP è una funzionalità di sicurezza avanzata che protegge l'ambiente di runtime delle applicazioni ed esegue il monitoraggio degli input dati per identificare, rilevare e bloccare gli attacchi. La RASP è molto utile per gestire la sicurezza avanzata delle applicazioni una volta comprese le aspettative in termini di complessità dell'implementazione e impatto sulle prestazioni.
- **Token di accesso privati (PAT).** Apple e altre aziende tecnologiche ripongono una sempre maggiore attenzione nei confronti della privacy degli utenti finali, offrendo metodi per verificare l'autenticità e affidabilità dei dispositivi che richiedono l'accesso, senza esporre i dati personali identificabili a rischi elevati. Il supporto WAAP di Apple PAT consente di ridurre l'utilizzo dei CAPTCHA o delle altre tecniche di rilevamento dei bot che causano fastidi o problemi in termini di esperienza utente. Apple PAT appartiene a un'iniziativa settoriale più ampia per la creazione di tecnologie in grado di preservare la privacy e garantire la condivisione dei dati degli utenti con parti selezionate, che possono eseguirne il trattamento, senza mettere a rischio le informazioni sensibili.
- **Automazione.** L'implementazione automatica degli aggiornamenti consente di ottimizzare la facilità d'uso e aggiungere valore al business.
- **Test di simulazione.** Test degli aggiornamenti delle regole prima dell'implementazione in produzione. I test di simulazione sono particolarmente efficaci se eseguiti sul traffico reale.

- **eBPF.** Funzione di Linux che consente l'esecuzione dei programmi nella sandbox del kernel del sistema operativo, in modo da gestire al meglio la sicurezza soprattutto negli ambienti cloud-native.

Considerazioni strategiche

Alla luce della rapida evoluzione delle tecnologie alla base di applicazioni Web e API, del cambiamento delle metodologie aziendali e delle capacità di adattamento dei criminali, gli acquirenti delle soluzioni di sicurezza devono analizzare in dettaglio la possibilità di soddisfare le esigenze aziendali dei prossimi tre-cinque anni. È possibile anche effettuare ulteriori considerazioni.

- **Offuscamento del rilevamento.** I criminali informatici sono sempre più abili nell'appropriarsi indebitamente di dati e prodotti, commettere frodi, creare danni o estorcere denaro alle aziende. Essi utilizzano strumenti sofisticati e tattiche intelligenti per attaccare gli obiettivi più redditizi. Quando le aziende di sicurezza riescono a identificare e contrastare gli attacchi, i criminali informatici riescono ad adattarsi e a variare le proprie tecniche fraudolente. I produttori di soluzioni WAAP dovrebbero investire nelle tecnologie di occultamento dei rilevamenti per utilizzare a lungo le proprie soluzioni di riduzione dei rischi. Inoltre, le strategie più efficaci in tal senso impediscono ai criminali di individuare l'intercettazione delle proprie attività, con la possibilità di azzerare le loro risorse. Esistono funzioni avanzate per la riduzione degli attacchi condotti mediante bot e frodi, tra cui l'uso delle tecnologie che impediscono ai criminali di completare lo sviluppo dei loro metodi fraudolenti.
- **Piattaforma.** I settori produttivi utilizzano piattaforme in grado di ridurre la complessità e dotate di funzionalità specializzate gestibili mediante un'interfaccia utente semplice, aspetto che non richiede uno sviluppo tecnico originale. Ad esempio, Shopify è una piattaforma di e-commerce che semplifica il processo di creazione di una nuova attività online. Caratteristiche come le informazioni sui clienti, l'inventario e l'elaborazione dei pagamenti vengono offerte come soluzione SaaS completa e pronta per l'uso. La sicurezza, comprese le protezioni WAF e DDoS di base, viene inclusa come funzionalità integrata della piattaforma. Questo scenario cambierà le esigenze e aspettative degli acquirenti delle soluzioni WAAP, imponendo ai produttori la necessità di adattamenti strategici.
- **Strategie di "spostamento a sinistra".** La necessità di implementare test e pratiche di sicurezza nelle prime fasi del ciclo di vita dello sviluppo del software non costituisce una novità. Il rilevamento delle vulnerabilità prima dell'invio in produzione impedisce ai criminali di individuare tali falle e sfruttarle adeguatamente. La diagnosi precoce e la correzione sono attività ancora più efficienti ed efficaci dal punto di vista dei costi. Tuttavia, negli ultimi anni è emerso il concetto di "spostamento a sinistra", vale a dire l'integrazione degli

strumenti tradizionali di post-produzione nei tool e flussi di lavoro degli sviluppatori. Ad esempio, l'utilizzo delle API per richiamare i test dinamici di sicurezza delle applicazioni (DAST) consente a DevOps di individuare e correggere le minacce in modo rapido e semplice. Inoltre, grazie alla possibilità, per i team DevOps, di lavorare in modo più veloce e usare microservizi, codice componibile, infrastructure as code (IaC) e altri metodi per ridurre i cicli di sviluppo, è ormai impossibile non utilizzare le strategie di "spostamento a sinistra".

- **Cambiamento delle identità.** La trasformazione di ogni elemento in una piattaforma, le strategie di "spostamento a sinistra" e l'aumento generale della consapevolezza della sicurezza, di cui tutti sono responsabili, stanno producendo un cambiamento negli acquirenti e nei responsabili delle decisioni. Gli sviluppatori, i team cloud e di rete e persino gli acquirenti della linea di business sono ormai coinvolti nel processo di acquisto delle WAAP. I produttori di soluzioni WAAP devono investire nella semplificazione, nell'automazione, nella protezione efficace e immediata e nella formazione di settore per supportare un'ampia gamma di acquirenti e responsabili delle decisioni.
- **GenAI.** L'introduzione della GenAI ha sollevato alcune preoccupazioni relative ai potenziali nuovi rischi che tale tecnologia potrebbe introdurre negli ambienti aziendali. Secondo una ricerca condotta da IDC fra gli acquirenti, le aziende stanno valutando l'aumento dei budget dedicati alla sicurezza delle applicazioni. I produttori di soluzioni WAAP offrono livelli molto variabili di attenzione e pianificazione nei confronti dei potenziali rischi legati alla GenAI. Ciò dipende da diversi fattori, fra cui:
  - Nuove minacce potenziali che sfruttano la GenAI per eludere le difese in modo più efficace
  - Possibili applicazioni delle tecnologie emergenti, come ad esempio la GenAI, per contrastare, ostacolare, rallentare o compromettere il funzionamento dei bot.
  - Necessità di implementare funzionalità, prodotti specializzati o possibilità di usare le difese esistenti. Infatti, le aziende hanno sviluppato funzionalità LLM, o sfruttano le soluzioni di terze parti, nelle proprie strategie applicative
  - Applicazioni potenziali della GenAI per l'ottimizzazione dell'efficienza e della produttività delle operazioni di sicurezza
  - Applicazioni potenziali dell'AI per l'ottimizzazione del rilevamento della sicurezza

Nel complesso, nonostante l'ampia gamma di funzionalità richieste e inserite nella definizione delle WAAP, IDC ha riscontrato caratteristiche di alto livello nelle soluzioni

prese in esame da questo MarketScape. La definizione di WAAP continuerà a cambiare a causa delle tecnologie emergenti e dell'evoluzione delle minacce. Esistono ancora margini di miglioramento in alcune aree funzionali e i produttori hanno delineato ampie tempistiche in tal senso. Anche se alcune applicazioni o esigenze eccezionali potrebbero imporre l'uso di prodotti specifici, i produttori di soluzioni WAAP hanno fatto passi da gigante verso la creazione di piattaforme complete, potenti e dotate di ogni funzionalità necessaria per garantire la protezione e le prestazioni delle applicazioni.

PROFILO RIEPILOGATIVO DEL PRODUTTORE

Questa sezione riassume le valutazioni espresse da IDC sul posizionamento dei produttori in MarketScape. Anche se ogni produttore viene valutato in base a ciascun criterio indicato nell'appendice, la descrizione seguente è da considerarsi un riepilogo dei punti di forza e debolezza dei singoli attori.

Akamai

Akamai è il leader di questo IDC MarketScape 2024 per le piattaforme aziendali WAAP a livello globale.

Si tratta di un fornitore globale di servizi di rete e sicurezza attraverso Akamai Connected Cloud, una piattaforma edge e cloud distribuita, che avvicina le applicazioni e le esperienze agli utenti contrastando le minacce. Akamai è specializzata nel mercato delle imprese e vanta una forte penetrazione fra le aziende Fortune 500. La linea di soluzioni di sicurezza dell'impresa comprende App & API Protector (AAP), una WAAP integrata, oltre a prodotti dedicati alla sicurezza delle API, mitigazione del DDoS, gestione dei bot, protezione degli account, WAF, protezione e conformità dal lato client, DNS e protezione del marchio. Akamai si occupa anche di sicurezza aziendale con soluzioni dedicate a ZTNA, microsegmentazione, firewall DNS, ricerca delle minacce e MFA.

Punti di forza

Caratteristiche

- Adaptive Security Engine (ASE) è in grado di adattarsi automaticamente per garantire un utilizzo affidabile delle regole predefinite. Secondo Akamai, il prodotto offre una protezione ottimale zero-day, migliora i rilevamenti di 2 volte e riduce i falsi positivi fino a 5 volte. Inoltre, gli aggiornamenti automatici garantiscono un utilizzo continuativo e semplice. ASE si basa sulla security intelligence di Akamai e

- offre una segnalazione dei falsi positivi per una correzione più facile e veloce di oltre il 50% dopo un giorno e del 75% entro una settimana.
- La suite completa WAAP offre un'esperienza di acquisto unica e una sicurezza semplificata e completa. È disponibile un singolo SKU per la soluzione WAAP, che offre componenti aggiuntivi e funzionalità avanzate o specifiche.
- Grazie a un'ampia gamma di componenti aggiuntivi e soluzioni specializzate è possibile soddisfare determinate esigenze, come ad esempio la protezione ATO, del marchio e dagli scraper (evento hype).
- Akamai offre un'infrastruttura edge/CDN su larga scala. La collocazione della protezione vicino all'utente offre una garanzia di prestazioni elevate.
- Il supporto dei flussi di lavoro DevOps supporta le strategie di "spostamento a sinistra" dei clienti aziendali. Il supporto per la gestione e distribuzione tramite API, CLI e Terraform offre una sicurezza ottimizzata senza rallentare il lavoro degli sviluppatori.
- Le integrazioni esistenti con gli strumenti di sicurezza consentono di ottimizzare la sinergia con l'architettura di protezione più estesa e di ottenere risultati migliori. La soluzione comprende connettori predefiniti per Splunk, Qradar e ArcSight e
- un approccio multimodale alla sicurezza delle API, che protegge il traffico API conosciuto sulla piattaforma e garantisce la sicurezza completa delle API in un secondo momento, se necessario.
- L'ampiezza delle funzionalità aggiuntive offerte insieme alla WAAP impedisce alla sicurezza di limitare le prestazioni dei sistemi. La linea di prodotti dell'azienda comprende soluzioni come ad esempio SiteShield, mPulse Lite, EdgeWorkers, Image & Video Manager e API Acceleration.
- Di recente, Akamai ha introdotto nuove funzionalità per la mitigazione dei DDoS a livello applicativo, tra cui il rilevamento degli short burst e la limitazione della velocità personalizzabile in base a indizi contestuali e granulari. Queste caratteristiche aiutano a contrastare numerosi attacchi DDoS, fra cui gli attacchi di livello applicativo.
- La soluzione comprende una vista unificata della telemetria di sicurezza che offre un'ampia analisi e visibilità della protezione, con la possibilità di eseguire esami dettagliati. Web Security Analytics è incluso in tutti i prodotti per la sicurezza delle applicazioni.
- La modalità di valutazione del prodotto consente di provare gli effetti delle modifiche alle regole applicandole sul traffico in tempo reale prima di implementare i cambiamenti. In questo modo è possibile creare nuove regole senza rischiare conseguenze sconosciute sul traffico di produzione.

Strategia

- Akamai ha annunciato piani per l'integrazione delle WAAP con gli strumenti di sicurezza adiacenti, come ad esempio la microsegmentazione. In questo modo sarà possibile integrare gli strumenti di sicurezza e fornire una difesa approfondita.
- Akamai sta sviluppando una serie di strategie atte a fornire protezione alla luce dell'aumento dell'utilizzo degli LLM. L'utilizzo degli strumenti esistenti per le nuove pratiche di sicurezza offre una notevole convenienza al cliente, anche se le protezioni specifiche per la GenAI offrono una specializzazione ancora superiore.
- L'azienda ha sviluppato piani aggressivi per espandersi nel settore dell'edge computing. Le opzioni per la protezione delle transazioni edge possono impedire che le minacce raggiungano i server di origine.
- Sono state fornite diverse prove dell'esecuzione di questa strategia, soprattutto per quanto riguarda la sicurezza delle API. La strategia di sicurezza delle API verrà completata con le acquisizioni di Noname Security e Neosec.
- L'azienda vanta una notevole esperienza nel campo delle acquisizioni strategiche, trasformando prodotti come Cyberfend, Neosec, Noname Security e Prolexic in una piattaforma coerente. Questi investimenti testimoniano l'impegno dell'azienda nei confronti della sicurezza dei clienti.
- Akamai sfrutta la telemetria per il monitoraggio dei progressi strategici, come ad esempio l'utilizzo/l'accettazione delle policy, la modalità automatica e lo stato della mitigazione. In questo modo, le strategie di sviluppo saranno in linea con la realtà operativa dei clienti.
- Le soluzioni WAAP relative alle origini in arrivo consentono di gestire i limiti della sicurezza CDN e proteggere il traffico est-ovest, non CDN e gli ambienti multicloud. Questa funzionalità verrà implementata a breve e sembra molto promettente.
- L'azienda offre diversi percorsi per il coinvolgimento dei clienti, come ad esempio conferenze, riunioni periodiche del consiglio consultivo, processi specifici.

Criticità

Caratteristiche

- Non è semplice, per i clienti, mettere a punto i motori di AI/ML. Ad esempio, non è possibile cambiare l'ordine delle regole, creando ritardi nella risposta ai falsi positivi e richiedendo la collaborazione con Akamai. Le eccezioni e soluzioni temporanee consentono di superare la complessità dell'ordinamento delle regole.

- I fattori di forma ridotti, come ad esempio i container e i sistemi serverless, creano limiti nel supporto ai clienti che intendono tenere sotto controllo l'infrastruttura di sicurezza. Attualmente, Akamai intende supportare Terraform e i controlli basati su API per l'implementazione e l'automazione.
- Le soluzioni WAAP di Akamai sono dotate di un prezzo molto elevato, a volte proibitivo per i responsabili delle decisioni aziendali. Tuttavia, le opzioni tariffarie di Akamai includono una protezione con commissione fissa e l'assenza di spese generali (Zero Overhead Fixed Fee, ZOFF), la tariffazione basata sulle richieste e la commissione per la protezione dai DDoS, che include l'eliminazione delle eccedenze per i picchi di traffico dovuti alle attività di DDoS.
- La soluzione non supporta gRPC, che potrebbe essere ideale in casi d'uso specializzati o settori specifici.

Strategia

- Le funzionalità e i componenti aggiuntivi specializzati e opzionali possono comportare costi aggiuntivi, aumentare il costo totale di proprietà (TCO) e ostacolare un'implementazione completa. Il traffico esterno al CDN (es. quello dei gateway delle API) richiede un costo aggiuntivo.
- La strategia di sviluppo delle WAAP prevede una condivisione nominale delle informazioni con la soluzione zero trust Akamai Enterprise Application Access (EAA). Le applicazioni Web possono trasformare le aziende e offrono una maggiore integrazione tra le linee di prodotti, in modo da supportare l'intera gamma delle applicazioni di accesso sicuro.
- Le soluzioni multiple (es. Account Protector, Brand Protector e Content Protector) producono una strategia antifrode frammentata che può aumentare la complessità della messaggistica.

Casi in cui consigliamo di prendere in considerazione Akamai

Akamai offre un'efficace serie di funzionalità di distribuzione, prestazioni e sicurezza, integrate in un unico servizio coerente. L'azienda concede in licenza le funzionalità avanzate e specializzate, come ad esempio i componenti aggiuntivi opzionali. Questa strategia consente ai clienti di investire in una soluzione su misura adatta alle proprie esigenze di sicurezza e distribuzione. Nel complesso, la soluzione WAAP di Akamai soddisfa tutti i requisiti di sicurezza, disponibilità, integrità e conformità imposti dalle aziende digitali su larga scala.

APPENDICE

Come leggere i grafici di IDC MarketScape

Ai fini della presente analisi, IDC ha suddiviso le principali attività necessarie per ottenere successo in due categorie: capacità e strategie.

L'asse Y indica le capacità attuali, l'assortimento dei servizi offerti dal produttore e la qualità dell'allineamento degli stessi con le esigenze del cliente. La categoria delle capacità indica le caratteristiche attuali dell'azienda e dei relativi prodotti. In questa categoria, gli analisti di IDC prendono in esame le metodiche utilizzate da un produttore per sviluppare o offrire funzionalità in grado di attuare una determinata strategia sul mercato.

L'asse X, quella delle strategie, indica la misura in cui la futura tattica del produttore è allineata con le esigenze dei clienti per i prossimi tre-cinque anni. La categoria delle strategie riguarda le decisioni di alto livello e le ipotesi in termini di offerte, segmentazione dei clienti, piani aziendali e mercato per i prossimi tre o cinque anni.

La dimensione degli indicatori relativi ai produttori di IDC MarketScape indica la quota di ciascun soggetto nel segmento di mercato in corso di valutazione.

Per ciascun criterio specifico, è stata eseguita la valutazione dei produttori su una scala da uno a cinque, in cui "tre" viene considerato il valore di base e una valutazione media, "cinque" la valutazione migliore e più rara e "uno" quella più bassa e altrettanto rara. Quindi, i criteri sono stati ponderati in base alla prospettiva degli analisti e alla conoscenza delle tendenze generali del mercato, in modo da fornire informazioni utili per il processo decisionale degli acquirenti IT. Le valutazioni per ciascun criterio sono state ponderate tra una valutazione "quantitativa" e una "qualitativa", secondo quanto appropriato e pertinente al criterio specifico.

La figura 1 indica una rappresentazione visiva di diversi fattori che si traducono in un posizionamento lungo ciascun asse. Le caratteristiche e funzionalità specifiche del prodotto esistente sono un importante componente dell'asse delle "caratteristiche", ma vengono presi in esame anche molti altri fattori. Allo stesso modo, l'asse delle "strategie" prende in considerazione i piani del produttore per gli sviluppi futuri delle soluzioni. Vengono presi in considerazione anche altri fattori, tra cui la forza dell'azienda nel complesso e i piani di accesso al mercato, dotati di un impatto a lungo termine sulla soluzione. IDC ha modificato di conseguenza il peso di questi criteri. In generale, la valutazione di ciascun produttore viene influenzata da diversi fattori. Consigliamo ai lettori di analizzare la figura 1 nel contesto fornito dai profili dei produttori.

Metodologia di IDC MarketScape

La scelta dei criteri, le ponderazioni e i punteggi dei produttori presenti in IDC MarketScape si basano sulle valutazioni condotte da IDC sul mercato e su produttori specifici. Gli analisti di IDC definiscono la gamma delle caratteristiche standard per la valutazione dei produttori attraverso discussioni strutturate, sondaggi e colloqui con leader di mercato, aziende secondarie e utenti finali. Le ponderazioni di mercato si basano sui colloqui con gli utenti, sui sondaggi fra gli acquirenti e sulle informazioni fornite dagli esperti di IDC in relazione a ciascun settore. Gli analisti di IDC elaborano i punteggi e le posizioni dei produttori di IDC MarketScape in base a sondaggi e colloqui dettagliati, informazioni pubbliche ed esperienze degli utenti finali, conducendo una valutazione precisa e coerente delle caratteristiche, del comportamento e delle capacità di ciascuno di essi.

Definizione del mercato

La WAAP è una soluzione di sicurezza convergente per la protezione attiva delle applicazioni incentrata sul WAF. Questo tipo di soluzioni uniscono diverse caratteristiche in una piattaforma di sicurezza unificata comprensiva di WAF, gestione dei bot, sicurezza API, mitigazione del DDoS e altre tecnologie di protezione. Tuttavia, il WAF è un elemento fondamentale e un componente integrale di una soluzione WAAP. Inoltre, le vendite una tantum dei componenti WAAP come soluzioni autonome non verranno conteggiate come un prodotto WAAP completo.

Componenti essenziali delle soluzioni WAAP

Web Application Firewall (firewall per le applicazioni Web)

I WAF consentono di monitorare, filtrare o bloccare le comunicazioni in transito da e verso un'applicazione Web. Un WAF può basarsi sulla rete o sul cloud e spesso viene implementato attraverso un proxy e posto davanti a una o più applicazioni Web. Il WAF è il componente principale di una soluzione WAAP.

Sicurezza delle API

Le soluzioni di sicurezza delle API consentono di proteggere le comunicazioni API da usi impropri, abusi ed exploit. Queste soluzioni offrono funzionalità di base, parziali o complete, come ad esempio acquisizione, convalida e applicazione degli schemi API, monitoraggio dinamico e adattivo del traffico, analisi dei modelli, rilevamento e prevenzione delle minacce (es. malware, exploit, iniezione di codice, bot, DDoS, frodi e usi impropri).

Potrebbero essere disponibili alcune funzionalità di protezione delle API come elementi predefiniti in un'offerta WAAP, come ad esempio le ispezioni del traffico API eseguibili

nello stesso punto di controllo di un WAF. Tuttavia, un'implementazione completa della sicurezza delle API può richiedere sensori e componenti aggiuntivi per garantire la visibilità e l'inventario di tutti gli endpoint API e, in ultima analisi, la protezione di tutte le comunicazioni legate alle API.

Gestione dei bot

La gestione dei bot garantisce l'integrità delle comunicazioni online limitando l'accesso ai soli utenti umani e consentendo le attività dei soli bot legittimi, controllati e approvati. Le soluzioni di gestione dei bot sfruttano numerosi segnali e approfondimenti su client, dispositivi, browser, identità dell'utente e comportamento, per poi combinarli con le analisi avanzate e individuare i bot più sofisticati ed elusivi. Queste soluzioni eseguono una divisione in categorie e un controllo dettagliato dell'intero ecosistema dei bot in base a profili di rischio, tipi di bot o bot specifici.

Il mercato completo della gestione dei bot offre soluzioni in grado di rispondere ai requisiti di sicurezza specifici imposti dai bot indesiderati. Esistono diversi livelli di integrazione tra le soluzioni WAAP. Il livello minimo, che offre il rilevamento e controllo dei bot, viene offerto da gran parte delle soluzioni WAAP, mentre le funzionalità avanzate vengono proposte come elementi aggiuntivi o upgrade in abbonamento.

Mitigazione del DDoS

Il mercato della mitigazione del DDoS comprende soluzioni in grado di rilevare e filtrare gli attacchi "distributed denial-of-service" (negazione del servizio distribuito). Anche se nei firewall, negli IPS e in altri prodotti di sicurezza sono presenti caratteristiche di difesa dai DDoS, le soluzioni specifiche consentono di gestire gli attacchi più estesi, complessi e innovativi. È possibile installare tali prodotti localmente, nel cloud o in entrambe le posizioni.

È possibile aggiungere diversi livelli di protezione a seconda della natura della soluzione o dell'implementazione WAAP. Gli elementi più avanzati, ad esempio le funzionalità aggiuntive o dedicate a tipi di attacchi specifici, sono disponibili come abbonamento aggiuntivo o aggiornamento.

Componenti estesi, avanzati e opzionali delle soluzioni WAAP

WAF lato client

Il WAF lato client (CSWAF) estende la visibilità e il controllo della sicurezza delle applicazioni agli script che vengono eseguiti nei browser degli utenti. Le soluzioni CSWAF variano marcatamente in termini di portata delle funzionalità. Le caratteristiche principali includono la visibilità, la valutazione e l'inventario degli script e delle comunicazioni. Il mercato delle funzioni di sicurezza avanzate, come ad esempio il rilevamento delle vulnerabilità, la crittografia, l'offuscamento del codice,

l'individuazione delle anomalie e minacce e l'applicazione delle policy, è molto frammentato.

Prevenzione delle frodi online

Tale attività interessa un'ampia gamma di soluzioni che operano in modo indipendente o congiunto per la protezione dei sistemi digitali dalle attività fraudolente o indesiderate. La prevenzione delle frodi online può richiedere soluzioni di gestione dell'identità, autenticazione forte, prova dell'identità, protezione dalle frodi dei pagamenti, rilevamento delle frodi nelle transazioni, prevenzione delle truffe aziendali e online.

Per quanto riguarda le soluzioni WAAP, le funzionalità di prevenzione delle frodi e degli usi impropri online fanno parte delle caratteristiche di gestione dei bot e consentono di contrastare gli schemi specifici delle attività fraudolente, come ad esempio l'acquisizione degli account o la frode dei nuovi account (detta anche frode degli account falsi). Per rilevare in modo completo frodi e altre azioni che indicano un abuso di applicazioni e API correttamente funzionanti, occorre eseguire approfondimenti sull'identità degli utenti, sulla telemetria a livello di client e dispositivo e sul comportamento dell'utente. Di conseguenza, esistono differenze significative tra le soluzioni WAAP in termini di capacità di rilevamento delle frodi e modalità di fornitura di queste funzionalità agli acquirenti.

ULTERIORI INFORMAZIONI

Ricerche correlate

- *Web Application and API Security Survey Presentation, 2024* (IDC n. US52509324, agosto 2024)
- *Identifying and Measuring the Costs of Cyberattacks Targeting Web Applications and APIs* (IDC n. US52025924, aprile 2024)
- *Market Analysis Perspective: Worldwide Active Application Security Market, 2023* (IDC n. US51332023, novembre 2023)
- *IDC TechBrief: Client-Side WAF* (IDC n. US51199423, settembre 2023)
- *Worldwide Application Protection and Availability Forecast, 2023–2027: Threat Escalation and New Frontiers* (IDC n. US51178423, settembre 2023)
- *Worldwide Application Protection and Availability Market Shares, 2022: Platforms Compete with Emerging Technologies* (IDC n. US51204923, settembre2023)
- *Tales of the Tape: WAF and API Protection Emerge as Security Essentials* (IDC n. US51187923, settembre 2023)

Sinossi

Questa ricerca di IDC fornisce una panoramica delle soluzioni WAAP in base alle caratteristiche, tenendo conto dei vantaggi offerti dai produttori, dalle partnership strategiche e tecniche, dalla proprietà intellettuale, dalle acquisizioni, dal costo totale di proprietà, dalla soddisfazione dei clienti e dai fattori di differenziazione della concorrenza. Le soluzioni WAAP offrono un approccio integrato che garantisce un accesso sicuro e ad alte prestazioni alle principali applicazioni Web e alle relative API. Il mercato si sta evolvendo rapidamente, richiedendo funzioni più avanzate rispetto alle capacità dei prodotti specifici per la riduzione del rischio. Per questo motivo, gli acquirenti delle soluzioni di sicurezza devono prendere in considerazione un'ampia gamma di funzionalità e approcci.

Secondo Christopher Rodriguez, direttore della ricerca del team sicurezza e attendibilità di IDC, "il mercato delle soluzioni WAAP si trova in una fase critica, poiché i produttori devono creare soluzioni in grado di fornire protezione nei confronti delle minacce online di nuova generazione e degli attacchi attuali. Allo stesso tempo, gli acquirenti aziendali devono gestire la pianificazione delle soluzioni WAAP alla luce della rapida evoluzione delle tecnologie".

INFORMAZIONI SU IDC

International Data Corporation (IDC) è il principale produttore al mondo di informazioni di mercato, servizi di consulenza ed eventi per il settore IT, delle telecomunicazioni e tecnologie per utenti finali. Grazie a oltre 1.300 analisti al lavoro in tutto il mondo, IDC offre competenze concrete a livello globale, continentale e nazionale su argomenti come tecnologia, benchmark e approvvigionamento delle soluzioni IT, opportunità e andamenti di settore in oltre 110 Paesi. Le analisi e gli approfondimenti di IDC consentono ai professionisti IT, ai dirigenti d'azienda e agli investitori di prendere decisioni basate sui fatti in materia di tecnologia, in modo da raggiungere i principali obiettivi di business. Fondata nel 1964, IDC è una società interamente controllata da International Data Group (IDG, Inc).

Sede centrale globale

140 Kendrick Street
Building B
Needham, MA 02494
USA
+1 508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com