La checklist per la valutazione delle soluzioni WAF

Uno strumento utile per trovare la giusta soluzione per le vostre esigenze di sicurezza delle applicazioni e delle API

Semplificate la ricerca del vendor di soluzioni WAF (Web Application Firewall) o WAAP (Web Application and API Protection) più appropriato. Questa checklist completa vi aiuta a valutare i provider di soluzioni WAF e WAAP in grado di soddisfare le vostre esigenze in termini di sicurezza e performance, nonché da un punto di vista operativo e finanziario.

Funzionalità per la sicurezza

Sicurezza delle applicazioni

- Assicuratevi una **protezione dalle 10 principali vulnerabilità riportate nell'elenco OWASP**, come gli attacchi SQL injection, XSS, LFI e SSRF. Verificate che sia possibile personalizzare e implementare automaticamente il sistema di protezione.
- Verificate se la soluzione sia in grado di controllare in modo proattivo il traffico proveniente da **indirizzi IP non affidabili** e di avvisarvi se **si verifica la violazione di un'eccezione precedente**.
- Valutate la **flessibilità degli elenchi di elementi consentiti/bloccati**: riuscite a correlare vari attributi come indirizzi IP, dati geografici, ASN e fingerprint TLS per creare policy efficaci?

Protezione dagli attacchi DDoS

- Verificate che il vendor sia in grado di offrire una **protezione per le applicazioni e le API dagli attacchi DDoS multilivello**, inclusi attacchi al DNS, ai livelli 3/4 e al livello 7.
- Verificate che la soluzione sia in grado di offrire una funzione di **rilevamento degli attacchi DDoS comportamentali** per la sicurezza delle applicazioni.
- Stabilite la granularità dei controlli per la **limitazione della velocità**. Questi controlli sono automatici o configurati manualmente? Queste misure possono proteggere dagli attacchi volumetrici e Slow POST?
- Esaminate le funzionalità in grado di **ridurre il carico di lavoro** durante gli attacchi al DDoS e migliorare le performance.
- Verificate i **costi aggiuntivi** che possono derivare dall'aumento del traffico durante gli attacchi DDoS.
- Verificate **che il sistema di protezione dagli attacchi DDoS al livello 7 sia automatizzato** per far risparmiare tempo e risorse al vostro team. I sistemi di **protezione si adattano** al profilo del traffico o alla tolleranza ai rischi della vostra azienda?

Protezione dagli attacchi zero-day

- Verificate che nella soluzione WAF siano presenti **sistemi di protezione dalle CVE note** in grado di adattarsi rapidamente per difendere dagli attacchi zero-day. Esaminate la capacità di **difesa dagli attacchi zero-day** e i relativi tempi di risposta.
- Verificate che i clienti della soluzione possano disporre di sistemi di **protezione da specifiche CVE**.

Protezione delle API

- Assicuratevi che la soluzione sia in grado di **proteggere gli endpoint delle API** da attacchi di tipo injection o DoS e da tentativi di violazione delle specifiche.
- Verificate che sia presente la funzione di **individuazione delle API**: è in grado di rilevare automaticamente le API nuove e modificate? Potete proteggerle facilmente con il sistema di protezione?
- Verificate che siano presenti funzioni di **rilevamento delle PII e generazione di avvisi** per salvaguardare i dati sensibili e prevenire le violazioni di dati.

Protezione dai bot

- Verificate che la soluzione WAF **sia in grado di rilevare e mitigare le minacce automatizzate** utilizzando una directory dei bot con le relative definizioni. Quali sono le dimensioni della directory dei bot? Con quale frequenza viene aggiornata con i bot nuovi e modificati?
- Verificate quali **definizioni dei bot** sono presenti nello strumento. Potete **creare definizioni dei bot personalizzate**?
- Controllate se la soluzione include un **meccanismo CAPTCHA o di verifica umana** tale da non interrompere le user experience. Il meccanismo di verifica/CAPTCHA richiede un'interazione con gli utenti finali prima di proseguire?

Automazione e intelligence sulle minacce

Intelligence sulle minacce

- Assicuratevi che il provider utilizzi **dati diretti** per l'intelligence sulle minacce per evitare ritardi dovuti a terze parti e potenziali manomissioni di dati.
- Verificate le dimensioni del **team addetto alla ricerca delle minacce** del provider e la rete globale di esperti di sicurezza che si occupano di monitorare i rischi emergenti.
- Valutate il **volume e l'importanza dei dati** elaborati dal database dell'intelligence. Sono inclusi dati ricavati da settori simili a quello in cui opera la vostra azienda o da organizzazioni frequentemente prese di mira dai criminali informatici?

Automazione

- Controllate se la soluzione WAF si basa su una **tecnologia obsoleta per il set di regole**. Usa tecnologie moderne e innovative come gli aggiornamenti automatizzati tramite l'euristica avanzata e l'apprendimento automatico?
- Assicuratevi che i set di regole vengano aggiornati automaticamente per **eliminare l'intervento manuale**. Gli aggiornamenti automatici vengono applicati a livello globale? In che modo è possibile rimuovere un aggiornamento applicato in precedenza o **provarlo sul traffico attuale**?
- Stabilite se la soluzione personalizza i sistemi di protezione in base al vostro ambiente senza richiedere l'intervento dell'utente. La soluzione **adatta continuamente** le policy di sicurezza in modo automatico in base al profilo del traffico della vostra organizzazione?
- Valutate il modo con cui la soluzione controlla i **falsi positivi**. In che modo la soluzione riesce a trovare un equilibrio riducendo i falsi positivi e minimizzando **l'interruzione del traffico legittimo**?

Visibilità e rapporti

Visibilità granulare

- Assicuratevi che la soluzione WAF sia in grado di fornire una **visibilità dettagliata sulle minacce** e sulle performance, con dashboard personalizzabili e rapporti sugli ambienti che utilizzano più soluzioni.
- Durante il funzionamento di una soluzione WAF, i team addetti alla sicurezza trascorrono la maggior parte del loro tempo alla console dei dati. Esaminate le opzioni di **personalizzazione**, le funzioni di analisi proattive e la **granularità dei rapporti** a cui potete accedere.
- Valutate la capacità della soluzione di **monitorare il traffico delle API** e delle applicazioni in modo efficace, rilevare gli abusi e fornire informazioni dettagliate sulla proliferazione delle API.

Analisi proattive e avvisi in tempo reale

- Verificate che siano disponibili funzionalità di invio di **avvisi quasi in tempo reale** al vostro team per informarlo sulle minacce più importanti. Gli avvisi devono essere personalizzabili in base a specifici criteri, come la gravità, l'origine o il tipo di attacco, per consentire una facile comprensione e una rapida risposta.
- Verificate che la soluzione sia in grado di fornire **informazioni pre-analizzate** sulla posizione, sul momento e sul modo con cui si verificano gli attacchi per ridurre il carico di lavoro che grava sul team addetto alla sicurezza. La soluzione deve anche **consigliare le successive operazioni da eseguire** per migliorare il vostro sistema di sicurezza.

Piattaforma e architettura

Portata globale

- Verificate che la soluzione WAF sia in grado di fornire l'accesso a servizi CDN o sull'edge della rete globale per migliorare le performance e la sicurezza. Esaminate la **disponibilità globale** della soluzione per proteggere le vostre sedi principali e quelle dei vostri clienti.

Supporto per ambienti cloud e ibridi

- Verificate che la soluzione sia **indipendente dal cloud** e in grado di supportare ambienti multicloud, ibridi e on-premise. Se la soluzione è basata su una CDN, assicuratevi che sia in grado di estendere la sua protezione oltre la CDN per una sicurezza al di fuori dell'edge.

Resilienza e failover

- Valutate la **resilienza della soluzione**: è in grado di eseguire il failover automaticamente per garantire la sua protezione in caso di disservizi o interruzioni?
- Esaminate i dati recenti sulle **interruzioni dei servizi e sui tempi di risposta del provider**.
- Stabilite se gli **accordi sul livello di servizio** (SLA) soddisfano le esigenze della vostra azienda.

Supporto e servizi gestiti

Accesso ai servizi e livelli di supporto inclusi

- Verificate i **livelli di supporto inclusi** e quelli disponibili a pagamento con la soluzione WAF.
- Verificate se è disponibile un servizio di **risposta agli incidenti 24/7**e se potete accedere direttamente al SOC (centro operativo per la sicurezza) durante gli attacchi.
- Assicuratevi che il vendor sia in grado di offrire **servizi di sicurezza totalmente gestiti** per colmare potenziali lacune presenti nelle vostre risorse interne, incluse le competenze necessarie per gestire gli attacchi, la configurazione o la turnazione del personale.

Integrazione e compatibilità del DevSecOps

Automazione di API, CLI e infrastrutture

- Verificate l'integrazione di **API, CLI e Terraform** per automatizzare e incorporare le funzioni di sicurezza desiderate nei vostri workflow di sviluppo. Il supporto di GitOps e di altri sistemi IaC (Infrastructure-as-Code) è fondamentale per applicare in modo coerente le policy di sicurezza nei vari ambienti.

Integrazione SIEM

- Assicuratevi che la soluzione WAF **si integri perfettamente con gli strumenti SIEM** come Splunk o QRadar per migliorare il monitoraggio, la generazione di rapporti e la risposta agli incidenti.

Efficienza e risultati aziendali

Scalabilità e performance

- Verificate la capacità della soluzione di **scalare automaticamente** per gestire elevati volumi di traffico senza peggiorare le performance. A che punto la soluzione crea problemi di latenza o diventa vulnerabile in caso di carico di lavoro elevato?
- Assicuratevi che sia stato predisposto uno **SLA (accordo sul livello di servizio) con disponibilità del 100%** e che la soluzione sia anche in grado di offrire opzioni di ottimizzazione delle performance, come il caching e l'accelerazione del traffico per migliorare le applicazioni.

Gestione unificata

- Verificate che il provider sia in grado di offrire un'interfaccia centralizzata per **gestire le policy di sicurezza in tutti gli ambienti** (cloud, on-premise e ibridi). Assicuratevi che la soluzione si integri con i vostri sistemi attuali e sia in grado di fornire un'experience eccellente per i team addetti alla sicurezza e allo sviluppo.

Convenienza

- Valutate la capacità della soluzione di **unificare soluzioni WAF, sistemi di difesa DDoS, gestione dei bot e funzioni di protezione delle API** scegliendo un solo vendor allo scopo di ridurre le difficoltà e i costi di gestione. Valutate l'equilibrio offerto tra efficacia in termini di sicurezza e costi operativi per stabilire il valore complessivo della soluzione.

Fiducia e affidabilità del vendor

Dati cronologici sui servizi e sulla stabilità

- Esaminate i dati cronologici del provider **relativi ai disservizi e alle interruzioni** che si sono verificati negli ultimi 5 anni.
- Verificate che l'azienda sia **stabile da un punto di vista finanziario**. È un'azienda redditizia? Da quanto tempo è attiva? A quali tipi di clienti si rivolge e di quali dimensioni?

Reputazione e recensioni

- Effettuate una ricerca per individuare le recensioni verificate e le testimonianze dei clienti al fine di capire se **il vendor è considerato affidabile** da organizzazioni che operano nel vostro stesso settore. I casi di utilizzo dei clienti attuali si allineano alle vostre esigenze?
- Verificate se la soluzione è **riconosciuta dagli analisti di settore** come Gartner e Forrester per le sue soluzioni per la protezione di applicazioni e API.
- Assicuratevi che, dopo aver discusso con il vendor, **siate sicuri** dei suoi tempi di risposta e del suo livello di supporto nel caso in cui si verifichino problemi una volta scelta la sua soluzione. Chiedete chi si occuperà del servizio di assistenza dopo la fase di onboarding iniziale.