Lista de verificação da avaliação final do WAF

Uma ferramenta para encontrar a solução certa para suas necessidades de segurança de aplicativos e APIs

Simplifique sua busca pelo fornecedor certo de firewall de aplicativos da web (WAF) ou proteção de aplicativos da web e API (WAAP). Use esta lista de verificação completa para avaliar provedores de WAF e WAAP, garantindo que a solução atenda às suas necessidades de segurança, desempenho, financeiras e operacionais.

Capacidades de segurança

Segurança de aplicativos

- Garanta **cobertura contra as 10 principais vulnerabilidades do OWASP**, como injeção de SQL, XSS, LFI e SSRF. Confirme se a proteção pode ser personalizada e implantada automaticamente.
- Avalie se sua solução controla proativamente o tráfego de **IPs com má reputação** e avisa sobre **abuso de uma exceção anterior**.
- Avalie a **flexibilidade de listas de permissão e bloqueio** — você pode correlacionar atributos como impressões digitais de IP, Geo, ASN e TLS para criar políticas eficazes?

Proteção contra DDoS

- Valide se o fornecedor oferece **proteção DDoS multicamadas** para aplicativos e APIs, incluindo DNS, Camada 3/4 e Camada 7.
- Confirme se a solução oferece **detecção comportamental de DDoS** para segurança de aplicativos.
- Determine a granularidade de controles de **limitação de taxa**. Elas são configuradas automaticamente ou manualmente? Essas medidas podem proteger contra ataques volumétricos e de postagem lenta?
- Analise as capacidades que **reduzem carga** durante ataques DDoS e melhore o desempenho.
- Entenda o potencial para **custos adicionais** do aumento de tráfego durante eventos DDoS.
- Garanta que a **proteção DDoS L7 seja automatizada** para economizar tempo e experiência da sua equipe. As **proteções são adaptativas** ao seu perfil de tráfego específico ou tolerância ao risco?

Proteção contra exploração de dia zero

- Confirme se o WAF tem **proteções existentes para CVEs conhecidos** e pode se ajustar rapidamente para se defender contra novas explorações de dia zero. Investigue o **histórico de defesa de dia zero** e tempos de resposta da solução.
- Determine se você tem **proteções contra CVEs específicos** como cliente.

Proteção de APIs

- Garanta que a solução **protege endpoints de API** contra ataques de injeção, DoS e violações de especificações.
- Verifique se há **descoberta de API** — posso detectar APIs novas e modificadas automaticamente? Com que facilidade você pode aplicar proteção a elas?
- Confirme **detecção e alertas de PII** para proteger dados confidenciais e evitar violações de dados.

Proteção contra bots

- Confirme se o WAF **detecta e atenua ameaças automatizadas** usando um diretório de bot e definições. Qual é a amplitude do diretório de bots? Com que frequência ele é atualizado com bots novos e modificados?
- Determine quais **definições de bot** existem na ferramenta. Você pode **criar suas próprias** definições de bot?
- Verifique se a solução inclui um **CAPTCHA ou mecanismo de verificação humana** que não atrapalhe a experiência do usuário. O CAPTCHA/verificação exige que seus usuários finais interajam com ele antes de prosseguir?

Inteligência de ameaças e automação

Inteligência de ameaças

- Garanta que o provedor utilize **dados primários** para inteligência de ameaças, evitando atrasos de terceiros e possível adulteração de dados.
- Verifique o tamanho da **equipe de caça a ameaças** do provedor e a rede global de especialistas em segurança que monitoram riscos emergentes.
- Avalie o **volume e relevância dos dados** processados pelo banco de dados de inteligência. Inclui dados de setores semelhantes ao seu ou de organizações frequentemente alvos de ataques cibernéticos?

Automação

- Verifique se o WAF depende de **tecnologia de conjunto de regras desatualizada**. Usa tecnologias avançadas e modernas, como atualizações automatizadas por meio de heurística avançada e aprendizado de máquina?
- Garanta que os conjuntos de regras sejam atualizados automaticamente para **eliminar intervenção manual**. As atualizações automáticas são aplicadas em nível global? Quais são suas opções para remover uma atualização aplicada anteriormente ou **testá-la em trânsito ativo**?
- Determine se a solução personaliza proteções para seu ambiente sem intervenção. A solução **ajusta automaticamente** políticas de segurança baseadas continuamente no perfil de tráfego ao vivo da sua organização?
- Avalie como a solução controla **falsos positivos**. Como ela equilibra a redução de falsos positivos com a minimização da **interrupção do tráfego válido**?

Visibilidade e geração de relatórios

Visibilidade granular

- Garanta que o WAF ofereça **visibilidade detalhada das ameaças** e desempenho, com painéis e relatórios personalizáveis que abrangem ambientes multissoluções.
- Ao operar um WAF, as equipes de segurança passam a maior parte do tempo no console de dados. Explore **personalizações**, recursos de análise proativa e **granularidade dos relatórios** ao seu dispor.
- Avalie a capacidade de a solução **monitorar tráfego de API** e tráfego de aplicativos de forma eficaz, detectar abusos e oferecer insights detalhados sobre a proliferação de APIs.

Alertas em tempo real e análise proativa

- Verifique se há recursos de **alerta em tempo quase real** que notificam sua equipe sobre ameaças críticas. Alertas devem ser personalizáveis com base em critérios específicos, como gravidade, origem ou tipo de ataque, para facilitar a compreensão e a resposta rápida.
- Procure a solução para produzir **insights pré-analisados** sobre onde, quando e como os ataques ocorrem para reduzir a carga sobre sua equipe de segurança. A solução também deve **recomendar os próximos passos** para melhorar sua postura de segurança.

Plataforma e arquitetura

Alcance global

- Confirme se o WAF oferece acesso a uma edge de rede global ou serviços CDN para melhor desempenho e segurança. Pesquise a **disponibilidade global** da solução para garantir cobertura para seus locais principais e os locais de seus clientes.

Suporte a nuvem e híbrido

- Verifique se a solução é **agnóstica em relação à nuvem** e capaz de oferecer suporte aos seus ambientes multicloud, híbridos e locais. Se for baseada em CDN, tenha certeza de que a solução possa estender a proteção além da CDN para segurança off-edge.

Resiliência e failover

- Avalie a **resiliência da solução** — posso fazer failover automaticamente para manter a proteção durante paralisações ou distúrbios?
- Analise as interrupções **recentes** de **serviço e a resposta do provedor**.
- Determine se os **acordos de nível de serviço** (SLAs) atendem às necessidades do seu negócio.

Suporte e serviços gerenciados

Suporte incluído e acesso a serviços

- Determine os **níveis de suporte incluídos** e disponíveis com a solução WAF a um custo adicional.
- Verifique se há **resposta a incidentes 24 horas por dia, 7 dias por semana** disponível e se você terá acesso direto ao centro de operações de segurança (SOC) durante os ataques.
- Garanta que o fornecedor ofereça **serviços de segurança totalmente gerenciados** para cobrir possíveis lacunas em seus recursos internos, incluindo experiência em lidar com ataques, configuração ou rotatividade de pessoal.

Integração e compatibilidade de DevSecOps

APIs, CLI e automação de infraestrutura

- Verifique se há integração de **APIs, CLI e Terraform** para automatizar e incorporar segurança em seus fluxos de trabalho de desenvolvimento. O suporte ao GitOps e outras estruturas de infraestrutura como código é crucial para a aplicação consistente de segurança em todos os ambientes.

Integração de SIEM

- Garanta que o WAF **integra-se perfeitamente com ferramentas de SIEM** como Splunk ou QRadar para monitoramento aprimorado, relatórios e resposta a incidentes.

Resultados e eficiência empresarial

Escalonamento e desempenho

- Confirme se a solução oferece **escalonamento automático** para lidar com grandes volumes de tráfego sem prejudicar o desempenho. Em que ponto a solução introduz latência ou se torna vulnerável sob carga pesada?
- Certifique-se de que há um SLA de **100% de disponibilidade** e avalie se a solução também pode fornecer melhorias de desempenho, como cache e aceleração de tráfego, para melhorar seus aplicativos.

Gerenciamento unificado

- Avalie se o provedor oferece uma interface de painel único para **gerenciar políticas de segurança em todos os ambientes**: nuvem, local e híbrido. Garanta que a solução seja integrável à sua pilha atual e ofereça uma experiência sem atritos para as equipes de segurança e desenvolvimento.

Economia

- Avalie a capacidade de a solução **unificar o gerenciamento de WAF, DDoS e bots e proteção de APIs** em um único fornecedor, reduzindo a complexidade e os custos de gerenciamento. Avalie o equilíbrio entre a eficácia da segurança e o custo operacional para determinar o valor geral.

Confiança e confiabilidade do fornecedor

Histórico de serviço e estabilidade

- Analise o **histórico de paralisações ou distúrbios de serviço** do provedor nos últimos 5 anos.
- Verifique se a empresa apresenta **estabilidade financeira**. É lucrativa? Há quanto tempo está no mercado? Que tamanhos e tipos de clientes ela atende?

Reputação e avaliações

- Pesquise avaliações verificadas e depoimentos de clientes para ver se há organizações semelhantes em seu setor que **confiam no fornecedor**. Os casos de uso dos clientes atuais estão alinhados com suas necessidades?
- Verifique se é **reconhecida por analistas da indústria** como Gartner e Forrester por suas soluções de proteção de aplicativos e API.
- Garanta que após as discussões com o fornecedor, **você se sinta confiante** na sua capacidade de resposta e suporte caso surjam problemas quando você se tornar um cliente. Pergunte quem dará suporte à sua conta após a integração inicial.