

## Akamai recebe a maior nota em dois de três casos de uso no relatório 2019 Gartner Critical Capabilities for Cloud Web Application Firewall Services



*O Gartner avaliou 12 importantes fornecedores de WAF baseados em nuvem. A Akamai recebeu as maiores notas para os casos de uso de aplicações de negócios essenciais para a Web (3,68/5) e de segurança de APIs (3,49/5).*

Para serem competitivas em meio às rápidas mudanças da economia digital atual, as organizações precisam disponibilizar suas aplicações de negócios por meio de websites e APIs. Essa necessidade vem promovendo uma implantação crescente e rápida de aplicações Web, APIs, aplicações móveis baseadas em APIs, dispositivos IoT e outras aplicações voltadas para o público. Todos estes casos de uso aumentam a complexidade e o risco e ampliam a área de ataque.

Além disso, eles aumentam os desafios.

As explorações de vulnerabilidade, como injeção de SQL, execução de arquivos mal-intencionados e scripts entre websites, podem reduzir ou até mesmo danificar o desempenho de um website. Mais insidiosamente, elas podem encaminhar a lógica da aplicação para um banco de dados. Assim, agentes mal-intencionados podem usá-la para comprometer e extrair dados das empresas.

Como medida de proteção contra este cenário de ameaças em evolução, muitas empresas implantam WAFs (Web Application Firewalls).

## Implantação de WAFs baseados em nuvem para proteção contra vários tipos de ameaça

Ao contrário dos firewalls tradicionais, que fornecem apenas proteção de servidor para servidor, os WAFs se posicionam entre os clientes e os servidores da Web. Eles foram projetados para inspecionar o tráfego HTTP antes que ele chegue às aplicações.

Os WAFs estão disponíveis como dispositivos implantados no local e também em serviços baseados em nuvem. No entanto, as tendências indicam que as empresas, quando viável, estão migrando para WAFs baseados em nuvem.

De acordo com o Gartner, "até 2023, mais de 30% das aplicações Web e APIs voltadas para o público serão protegidas por serviços de proteção de aplicações Web e APIs (WAAP) na nuvem que combinam proteção contra ataques distribuídos de negação de serviço (DDoS), atenuação de bots, proteção de APIs e WAFs. Isso representa um aumento em relação aos menos de 10% atuais."<sup>1</sup>

Os WAFs baseados em nuvem normalmente oferecem maior escala e flexibilidade do que os dispositivos localizados em um data center. Em geral, eles têm ampla visibilidade do tráfego da Internet e podem identificar rapidamente ameaças emergentes e adaptar os meios de proteção apropriadamente.

O WAF da Akamai recebe a maior nota em dois de três importantes casos de uso:

- Maior nota para aplicações de negócios essenciais para a Web (3,68 de 5)
- Maior nota para segurança de APIs (3,49 de 5)
- Terceira maior nota para aplicações Web voltadas para o público (3,60 de 5)

## A Akamai recebe a maior nota em dois de três casos de uso

### Proteção de websites e aplicações Web contra tempo de inatividade e roubo de dados

O Kona Site Defender, uma solução WAF de nível empresarial da Akamai, utiliza um conjunto de ferramentas multicamadas e sempre ativas para proteger websites e APIs contra ataques sofisticados de DDoS, aplicações Web e diretos na origem.

Implantado na maior plataforma de entrega em nuvem do mundo, com mais de 260 mil servidores em 131 países, o Kona Site Defender autentica o tráfego válido na borda, com incomparável capacidade de bloquear ataques.

Esse tipo de proteção de desempenho foi criado para que os clientes possam entregar excelentes experiências para o usuário final, até mesmo sob ataque. Além disso, as organizações podem inovar agressivamente suas ofertas para Web e dispositivos móveis, sem muitas das distrações de segurança que retardam o lançamento no mercado.

#### Recursos do Kona Site Defender:

##### Plataforma de nuvem global

Desenvolvido com base na maior plataforma de entrega em nuvem do mundo, o Kona Site Defender foi projetado para deter ataques na borda antes que eles alcancem as aplicações.

##### Proteção contra DDoS

O Kona Site Defender minimiza possíveis tempos de inatividade, além de proteger as aplicações contra os maiores ataques DDoS.

##### Web Application Firewall

Protege contra ameaças à camada de aplicações com um conjunto de regras automatizado e altamente personalizável.

##### Proteção de APIs

Proteções voltadas para APIs contra ataques DDoS e ataques baseados em parâmetros, capazes de configurar proteções e relatar eventos de segurança por API.

##### Atualizações de regras

Com inigualável visibilidade dos mais recentes ataques, a Akamai atualiza os conjuntos de regras de segurança de forma contínua e transparente, deixando você no controle da ativação.

##### Patches virtuais

As regras personalizáveis permitem que você forneça um patch virtual para proteger rapidamente as aplicações ou adaptar a proteção ao tráfego do seu website.

##### 100% de disponibilidade e tempo de atividade

Uma plataforma altamente resiliente e de autorrecuperação é acompanhada de um SLA (Acordo de Nível de Serviço) com 100% de tempo de atividade e site failover para manter seu website ativo, mesmo em caso de falha dos seus servidores.

##### SureRoute

Atenua os problemas de rede que fogem do seu controle para melhorar o desempenho e a disponibilidade e fornecer aos usuários uma rota ideal até o seu website.

##### Desempenho aprimorado

O armazenamento em cache, os recursos avançados de transferência e a otimização de TCP foram projetados para melhorar o desempenho do website para os usuários, até mesmo sob os maiores ataques.

##### APIs de gerenciamento

Integre controles de segurança ao desenvolvimento de software e ao pipeline de entrega.

##### Análise de segurança avançada da Web

Ajuda a manter a configuração de segurança ideal, adaptada às suas necessidades específicas de negócios.

## A Akamai recebe a maior nota em dois de três casos de uso

### Acesse o relatório completo, uma cortesia da Akamai

O relatório 2019 Gartner Critical Capabilities for Cloud Web Application Firewall Services contém informações valiosas para os líderes de segurança que estão avaliando as proteções por WAFs para suas aplicações Web e móveis. Ele inclui as principais descobertas, recomendações, premissas de planejamento estratégico e muito mais.

O relatório inclui também a classificação de 1 a 5 do Gartner em relação à capacidade de cada vendedor para entregar 11 recursos essenciais de WAF. O Gartner avaliou cada um desses recursos em termos de importância relativa para chegar às notas atribuídas aos casos de uso.

No relatório completo, é possível ver a nota de cada fornecedor para cada recurso essencial. Você também poderá ler explicações detalhadas sobre a capacidade de entrega de cada fornecedor dos cinco recursos essenciais considerados mais importantes pelo Gartner ao avaliar os serviços de WAF. O relatório está disponível hoje, como cortesia da Akamai.



Leia agora o relatório Critical Capabilities for Cloud Web Application Firewall Services do Gartner. **Baixar relatório.**

#### 1. Relatório 2019 Gartner Critical Capabilities for Cloud Web Application Firewall Services

Gartner Research, Critical Capabilities for Cloud Web Application Firewall Services, 29 de outubro de 2019, Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur, John Watts

O Gartner não protege fornecedores, produtos nem serviços ilustrados nestas publicações de pesquisa, bem como não recomenda que usuários de tecnologias escolham somente fornecedores com as classificações mais altas ou outras designações. As publicações de pesquisa do Gartner consistem em opiniões da organização de pesquisa do Gartner e não devem ser interpretadas como declarações de fatos. O Gartner se isenta de todas as garantias, expressas ou implícitas, com relação a esta pesquisa, incluindo quaisquer garantias de comerciabilidade ou adequação a uma finalidade específica.



A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A plataforma de borda inteligente da Akamai engloba tudo, desde a empresa até a nuvem, para que os clientes e suas empresas possam ser rápidos e inteligentes e estar protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a obter vantagem competitiva por meio de soluções ágeis que ampliem o poder de suas arquiteturas compostas por várias nuvens. A Akamai mantém as decisões, aplicações e experiências mais próximas dos usuários, e os ataques e as ameaças cada vez mais distantes. O portfólio de soluções de segurança de borda, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeo da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, sete dias por semana. Para saber por que as principais marcas mundiais confiam na Akamai, acesse [www.akamai.com](http://www.akamai.com), [blogs.akamai.com](http://blogs.akamai.com), ou [@Akamai](https://twitter.com/Akamai) no Twitter. Nossas informações de contato globais podem ser encontradas em [www.akamai.com/locations](http://www.akamai.com/locations). Publicado em 11/19.