# CONHEÇA AS PRINCIPAIS SOLUÇÕES DA AKAMAI QUE SÃO DESTAQUES NO PORTFOLIO DE SOLUÇÕES DA ADD VALUE

Akamai | addvalue


# KONA SITE DEFENDER

## Proteção WAF e DDoS na Edge

Proteja websites, aplicações Web e APIs contra tempo de inatividade e roubo de dados

O Kona Site Defender oferece segurança de aplicação na Edge, mais próximo dos invasores e mais longe de suas aplicações. Com 178 bilhões de acionadores de regra de WAF por dia, a Akamai aproveita a visibilidade incomparável dos ataques para oferecer proteções de WAF organizadas e altamente precisas que acompanham as ameaças mais recentes. Proteções flexíveis ajudam a proteger todo o seu espaço de ocupação da aplicação e a responder às mudanças nas exigências de negócios, incluindo APIs e migração para a nuvem, com custos de gerenciamento drasticamente reduzidos.

### Visão geral

A confiança do consumidor na segurança, na disponibilidade e na marca provavelmente nunca esteve tão fragilizada. Se ocorrer uma violação de dados bem-sucedida, pode-se perder a confiança interna nas operações, na cadeia de suprimentos e na integridade dos dados. Para ganhar e manter a confiança, as organizações devem reduzir os riscos operacionais e de negócios das ameaças mais recentes, produzindo apenas os mais altos resultados de segurança. O Kona Site Defender, o firewall de aplicações Web líder do setor e baseado em nuvem, aproveita a visibilidade da Akamai Intelligent Edge Platform para impedir os mais sofisticados ataques DDoS (Distributed Denial- of-Service), ataques baseados em APIs e em aplicações Web e proteger o que é mais importante: a confiança.

### Firewall avançado e inteligência contra ameaças

O Kona Site Defender inclui um vasto conjunto de regras de firewall de camada de aplicação configuráveis e predefinidas que são constantemente atualizadas pela pesquisa de ameaças da Akamai. Essa inteligência, fruto do aprendizado de máquina e da análise humana, fornece a detecção mais avançada e precisa. As regras personalizadas e os perfis de proteção automatizados foram projetados para fornecer a flexibilidade e a escala para englobar todos os conjuntos de recursos da Web e de APIs, melhorar a eficiência operacional e proporcionar mais rapidez no tempo de retorno.

## Proteção contra DDoS para a camada de rede e de aplicação

A plataforma de borda inteligente globalmente distribuída da Akamai foi projetada como um proxy reverso para aceitar apenas o tráfego pelas portas 80 e 443. Todos os ataques DDoS de camada de rede são instantaneamente descartados na borda com um SLA (Acordo de Nível de Serviço) de zero segundo. O Kona Site Defender absorve os ataques DDoS na camada de aplicação, inclusive os ataques lançados por meio de APIs, e, simultaneamente, concede acesso aos usuários legítimos. Os ataques DDoS contra sua infraestrutura de DNS também podem ser atenuados com a solução de DNS de borda da Akamai.

## Detecção e segurança automáticas de API

O Kona Site Defender inspeciona automaticamente o tráfego de API que atravessa a plataforma da Akamai para fornecer uma lista de APIs não identificadas previamente, incluindo definições, características e pontos de extremidade de APIs. Com essa visibilidade, as equipes de segurança conseguem acompanhar as definições em constante mudança e registrar, com facilidade, as APIs para proteção. Com o Kona Site Defender, os modelos positivos e negativos de segurança protegem as APIs contra chamadas mal-intencionadas. O modelo negativo de segurança analisa e inspeciona automaticamente o tráfego XML e JSON em busca de ataques de aplicações, enquanto o modelo positivo permite apenas o tráfego de API predefinido. Além disso, é possível produzir análises, relatórios e alertas em tempo real no nível de API.

## Integração com processos de CI/CD

Com o Kona Site Defender, as organizações podem integrar proteções de WAF a processos de desenvolvimento ágil, gerenciando e vinculando, de maneira programática, controles de segurança no início do ciclo de desenvolvimento. As equipes de desenvolvedores, segurança e operações podem aproveitar uma ampla variedade de APIs de gerenciamento e a CLI (Command-Line Interface) para integrar tarefas de configuração de segurança ao processo de CI/CD, o que possibilita práticas recomendadas de segurança por projeto e o paradigma "shift left".

## Recursos

**Firewall de aplicação:** dois modos de operação, autogerenciado e gerenciado pela Akamai, oferecem o máximo de flexibilidade e cobertura. As regras autogerenciadas (Kona Rule Set) contam com controles de segurança totalmente personalizáveis, enquanto as regras gerenciadas pela Akamai (grupos de ataque automatizados) eliminam totalmente a necessidade de configurar e atualizar regras. As regras gerenciadas pela Akamai também têm lógica de detecção avançada que se ajusta dinamicamente com base nas características das solicitações recebidas. Com duas opções de gerenciamento, as empresas podem proteger 50% mais aplicações e APIs com 50% menos esforço.

**Proteção contra DoS (controles de taxa):** proteja-se contra taxas excessivas de solicitação e ataques DoS (Denial-of-Service), monitorando e controlando as taxas de solicitações. Os infratores são automaticamente bloqueados para proteger as origens do website.

**Análise avançada de segurança na Web:** acesse a telemetria detalhada de ataques e a análise de eventos de segurança para avaliar quais alterações são necessárias para melhorar as proteções de segurança e otimizar as configurações que são personalizadas de acordo com as necessidades específicas de sua empresa.

**Firewall de borda de rede (IP/Geo):** os controles IP/Geo permitem bloquear ou permitir o tráfego proveniente de uma sub-rede, uma área geográfica ou um IP específico. Isso permite bloquear solicitações mal-intencionadas de endereços IP específicos ou o tráfego do Tor (The Onion Router), que os hackers usam para ocultar sua identidade.

**CLI e APIs abertas:** as configurações de segurança são totalmente acessíveis, editáveis e auditáveis por meio da CLI e de APIs abertas, dando a você a liberdade de integrar e personalizar como desejar.

**Regras personalizadas:** o Kona Site Defender oferece um criador de regras personalizadas para gerar, com rapidez e facilidade, regras personalizadas que podem ser usadas para lidar com cenários exclusivos não cobertos por regras padrão ou para corrigir rapidamente novas vulnerabilidades de websites.

**Ações de resposta:** crie e forneça uma ampla gama de ações de resposta, incluindo respostas totalmente personalizadas. Você pode enviar mensagens de erro personalizadas, páginas da marca com seu próprio logotipo ou até mesmo definir e fornecer respostas baseadas em HTML, XML ou JSON, dependendo de suas necessidades.

**Modo de avaliação:** avalie facilmente regras de WAF novas ou atualizadas sobre o tráfego dinâmico, em conjunto com proteções ativas, para atualizar perfeitamente para fazer upgrade para as proteções mais recentes. Embora a Akamai atualize as regras de WAF de maneira contínua e transparente, você tem controle total da avaliação e da ativação.

**Desempenho e entrega:** escalone continuamente para atender às demandas de tráfego à medida que elas variam com o tempo, distribua recursos de CPU e memória conforme a necessidade, entregue, na borda, conteúdos armazenados em cache e forneça proteção contínua, sem interrupções, para garantir o mais alto nível de desempenho e entrega.

**Geração de relatórios:** as ferramentas de geração de relatórios de segurança da Web monitoram e avaliam continuamente a eficácia de suas proteções. É possível criar relatórios em tempo real para monitorar atividades diárias, investigar ataques por tipo e política de segurança, além de visualizar relatórios sobre APIs direcionadas, tráfego de DoS e muito mais.

**Alertas em tempo real:** crie alertas por e-mail em tempo real usando filtros estáticos e limites que podem ser facilmente configurados para notificar apenas destinatários específicos.

**Site Shield:** uma camada adicional de proteção que ajuda a impedir que os invasores contornem as proteções na nuvem e atinjam sua infraestrutura de origem.

**Integração de SIEM:** os conectores pré-integrados permitem usar aplicações de SIEM locais e baseadas em nuvem, tais como Splunk, QRadar, ArcSight e muito mais.

## Outras soluções para aumentar a proteção

**Client Reputation:** as pontuações de reputação baseadas em inteligência baseiam-se na visibilidade da Akamai sobre o comportamento anterior de endereços IP individuais e compartilhados.

**Bot Manager:** detecte, identifique, categorize e gerencie os bots que estão acessando seu website. Os algoritmos de aprendizado de máquina usam a telemetria de comportamento humano e de bots para permitir bots "bons" e, ao mesmo tempo, impedir que bots mal-intencionados executem ataques, como abuso de credenciais e tomada de controle de contas.

**Managed Security Services:** intensifique ou transfira o gerenciamento de segurança, o monitoramento e a atenuação de ameaças para os especialistas em segurança da Akamai.

**Page Integrity Manager:** proteja websites contra as ameaças de JavaScript, tais como skimming da Web, formjacking e ataques Magecart, identificando recursos vulneráveis, detectando comportamentos suspeitos e bloqueando atividades mal-intencionadas.

**Os benefícios dos produtos da Akamai não param por aí.**

**Clique no botão abaixo e entre em contato com o nosso time de especialistas e, fique por dentro de todos os benefícios e diferenciais dos produtos da Akamai.**

**Fale com o Especialista**

**Nos siga nas redes sociais e fique por dentro de todas as novidades!**

addvalue

**FALE CONOSCO**