

App & API Protector

No mundo conectado de hoje, proteger aplicativos da Web e APIs contra a ampla variedade de ameaças emergentes e em desenvolvimento é fundamental para que haja sucesso nos negócios. No entanto, a proteção de interações digitais em meio a jornadas de migração para a nuvem, novas práticas de DevOps e aplicativos em constante mudança traz novas complexidades e desafios.

Com a implantação de uma solução abrangente de proteção de aplicativos da Web e APIs (WAAP), sua postura de segurança é fortalecida com a atualização adaptativa de proteções e da divulgação proativa de insights sobre vulnerabilidades visadas.

O **Akamai App & API Protector** é uma solução unificada que reúne diversas tecnologias de segurança, incluindo firewall de aplicativos da Web (WAF), mitigação de bots, proteções de APIs e defesa contra negação de serviço distribuída (DDoS). O App & API Protector é conhecido como uma solução avançada de WAAP para identificar e mitigar ameaças rapidamente além do WAF tradicional, protegendo patrimônios digitais inteiros contra ataques multidimensionais. A plataforma é fácil de implementar e usar, fornece visibilidade abrangente e implementa automaticamente proteções personalizadas e atualizadas através do Akamai Adaptive Security Engine.

O poder da segurança adaptativa

O App & API Protector vai além de conjuntos de regras com o Adaptive Security Engine. Com essa tecnologia inovadora, as defesas de segurança são atualizadas contínua e automaticamente, com recomendações de políticas personalizadas implementadas em um só clique. O Adaptive Security Engine oferece proteção moderna ao combinar aprendizado de máquina, inteligência de segurança em tempo real, automação avançada e insights de mais de 400 profissionais de segurança e pesquisadores de ameaças. O Adaptive Security Engine é diferenciado porque:

- Analisa as características de cada solicitação em tempo real na edge para uma detecção mais rápida
- Aprende padrões de ataque utilizando dados locais e globais para fazer ajustes de proteção específicos para o cliente
- Adapta-se a ameaças futuras, o que garante a atualização das defesas mesmo com a evolução dos ataques

O Adaptive Security Engine alivia a sobrecarga de ajustes manuais e demorados com atualizações sem necessidade de intervenção, proporcionando uma experiência quase totalmente automatizada. No lançamento, comprovou-se que essa tecnologia aumenta as detecções em duas vezes e reduz os falsos positivos em cinco vezes. As atualizações recentes dos nossos algoritmos baseados em aprendizado de máquina agora reduzem os falsos positivos em mais 4 vezes. Os profissionais de segurança podem ser o destaque novamente, com mais tempo para se concentrar na entrega de operações comerciais digitais seguras e voltadas para o cliente.

Benefícios para os seus negócios

-  **Detecção confiável de ataques**
Acompanhe o cenário de ameaças e proteja-se contra ameaças consolidadas e emergentes, incluindo DDoS, botnets, injeções, ataques a APIs e mais
-  **Um único produto, ampla proteção**
Maximize seu investimento em segurança com uma solução que inclui WAAP, visibilidade e mitigação de bots, proteção contra DDoS, conectores de gerenciamento de informações e eventos de segurança (SIEM), otimização da Web, computação em nuvem e aceleração de APIs, entre outros
-  **Segurança prática**
Reduza a manutenção manual e demorada com atualizações automáticas e recomendações proativas de autoajuste impulsionadas pelo Akamai Adaptive Security Engine
-  **Facilidade de uso**
Use o design aprimorado da IU para simplificar a integração e as operações abrangentes de segurança, que contam com o suporte de guias de configuração e solução de problemas
-  **Visibilidade unificada**
Analisar todo o seu escopo de métricas de segurança em um único painel ou relatório de descoberta proativa por meio da telemetria compartilhada das soluções de segurança da Akamai



Novidade: Behavioral DDoS Engine

O novo Behavioral DDoS Engine fortalece e simplifica a defesa contra DDoS na camada do aplicativo e é alimentado por aprendizado de máquina. Os algoritmos de detecção comportamental e baseada em anomalias do Behavioral DDoS Engine analisam várias dimensões de tráfego, como país, impressão digital de rede e outros atributos de solicitação HTTPS para criar proteções personalizadas e fornecer uma abordagem prática contra ataques de DDoS na camada do aplicativo.

O uso de aprendizado de máquina pelo Behavioral DDoS Engine melhora a eficácia e a tomada de decisões sobre as dimensões do tráfego para uso na criação de perfis e referências de tráfego. O mecanismo de pontuação de diferentes níveis de sensibilidade considera o apetite ao risco de sua empresa para detectar ataques e minimizar falsos positivos.

Indo além de conjuntos de regras, o Akamai App & API Protector é alimentado pelo Adaptive Security Engine.

Deteção avançada de ataques — Com o crescimento do seu ambiente digital, também aumentam a profundidade e a amplitude de suas defesas enquanto cliente da Akamai. Além das atualizações automáticas e do autoajuste adaptável que o Adaptive Security Engine oferece, o App & API Protector fornece deteção avançada e reconhecida por analistas de DDoS, bots, malware e outros vetores de ataque. Valide suas proteções da Akamai contra CVEs emergentes e avançados com nossa ferramenta de pesquisa de ameaças.

Segurança de aplicativos — O App & API Protector apresenta um conjunto completo de defesas e personalizações para permitir que a segurança seja adaptada às necessidades da sua organização. Recursos eficazes, como o Client Reputation, listas de rede, deteção de novos ataques e mais, dão a você a vantagem contra adversários, ao mesmo tempo em que simplificam as operações de segurança. As defesas avançadas e fornecidas na camada do aplicativo pela solução de WAAP da Akamai detêm DDoS, injeções de SQL, cross-site scripting, inclusão de arquivo local, falsificação de solicitação do lado do servidor e outros vetores de ataque.

Proteção contra DDoS e controles granulares de taxa — Reconhecido como uma solução contra DDoS líder de mercado, o App & API Protector fornece proteção contra DDoS em várias frentes. Ele começa detendo ataques de DDoS na camada da rede na edge para mitigação de riscos e economia de recursos. Em seguida, ele detecta e mitiga automaticamente os sofisticados ataques de DDoS da camada 7 na edge para proteção prática e em tempo real contra o cenário em evolução das ameaças de DDoS. Os controles granulares de taxa personalizam sua defesa contra DDoS especificamente de acordo com seus perfis de tráfego e ataque.

Visibilidade e mitigação de bots — Obtenha visibilidade em tempo real do tráfego de bots com acesso ao amplo diretório da Akamai, com mais de 1.750 bots conhecidos. Investigue análises da Web distorcidas, evite a sobrecarga de origem e crie suas próprias definições de bots para permitir o acesso a bots de terceiros e de parceiros sem obstrução. Controles de bot expandidos, incluindo deteção de falsificação de navegadores, ações condicionais e desafios de criptografia, agora estão incluídos no App & API Protector.

OWASP Top 10

A Akamai mitiga os riscos do OWASP Top 10 e do OWASP API Security Top 10. Saiba como o App & API Protector e a segurança da Akamai protegem os clientes contra ameaças expressivas, comuns ou emergentes.

Para saber mais sobre as proteções da Akamai contra os riscos do OWASP Top 10, [baixe o white paper](#).



Proteções de APIs — A proteção de APIs líder do setor oferecida pela Akamai aumenta sua segurança através de visibilidade do tráfego em todo o seu patrimônio digital, proativamente revelando vulnerabilidades, identificando alterações no ambiente e protegendo contra ataques ocultos. Com os recursos de API do App & API Protector, você pode:

- Descobrir automaticamente uma variedade completa de APIs conhecidas, desconhecidas e variáveis em todo o seu tráfego da Web, incluindo os respectivos pontos de extremidade, definições e perfis de tráfego
- Registrar facilmente APIs recém-descobertas com apenas alguns cliques
- Garantir a proteção de APIs contra DDoS, injeção mal-intencionada, ataques de abuso de credenciais e violações de especificações de APIs
- Controlar o processamento de dados confidenciais com o recurso do App & API Protector de geração de relatórios sobre informações de identificação pessoal para manter a conformidade

Desempenho e mais a partir da maior rede global — A plataforma da Akamai oferece aos clientes uma vantagem competitiva devido à sua escala global incomparável, oferecendo visibilidade em tempo real de uma parte significativa do tráfego global da Internet. Esse vasto conjunto de dados permite que a Akamai forneça inteligência prática, ajudando as organizações a se manter à frente das ameaças de segurança em evolução e permitindo detecção e mitigação mais rápidas de ataques em vários ambientes. A plataforma também fornece um aumento de desempenho comprovado e um SLA (Acordo de Nível de Serviço) de 100% de disponibilidade.

Proteção contra malware — Este módulo complementar oferece verificação de arquivos na edge, antes do seu upload, para detectar malware e impedi-lo de invadir seus sistemas corporativos através do envio de arquivos maliciosos. Sem a necessidade da configuração adicional de apps ou APIs, você economiza tempo sem ter de configurar a proteção de cada sistema individualmente.

Integração Simple Start — Ferramentas de segurança excelentes só funcionam se você as usa. A Akamai se dedica ao desenvolvimento de uma plataforma fácil de usar que proporciona produtividade e defesas eficazes. Você pode se integrar rapidamente com nosso Simple Start ou aplicar proteções a novos aplicativos com apenas alguns cliques.

Painéis, alertas e ferramentas de geração de relatórios — O Web Security Analytics é o painel de telemetria de ataques detalhado da Akamai. Nele, você pode analisar eventos de segurança, criar alertas de e-mail em tempo real usando filtros e limites estáticos e utilizar ferramentas personalizáveis de geração de relatórios que monitoram e avaliam continuamente a eficácia de suas proteções na plataforma da Akamai.

Integrações de DevOps — Integre perfeitamente a segurança aos fluxos de trabalho de DevOps com GitOps, garantindo que a segurança se alinhe ao desenvolvimento acelerado. As APIs da Akamai, disponíveis através da CLI ou do Terraform, permitem o gerenciamento completo do App & API Protector via código e correspondem a todas as ações disponíveis na interface do usuário.

Integrações de SIEM — Também estão disponíveis APIs de SIEM, e conectores pré-desenvolvidos para Splunk, QRadar, ArcSight e outros estão incluídos automaticamente no App & API Protector.



Recursos integrados – Para aumentar a visibilidade e o desempenho, agora o App & API Protector conta com muitos dos produtos mais adorados pelos clientes da Akamai, incluindo:

- Site Shield: evite que os invasores burlam as proteções baseadas na nuvem e ataquem sua infraestrutura de origem
- mPulse Lite: obtenha ampla visibilidade do comportamento dos usuários, gerencie problemas de desempenho em tempo real e meça os impactos de mudanças digitais na receita
- EdgeWorkers: conheça as vantagens da computação sem servidor, que incluem mais rapidez no tempo de lançamento no mercado e execução de lógica mais próxima dos usuários finais
- Image & Video Manager: otimize imagens e vídeos de maneira inteligente com a combinação ideal entre qualidade, formato e tamanho
- API Acceleration: aprimore o desempenho de suas APIs através da simplificação do gerenciamento de acesso, do dimensionamento em caso de picos por alta demanda e do aprimoramento da segurança de APIs.

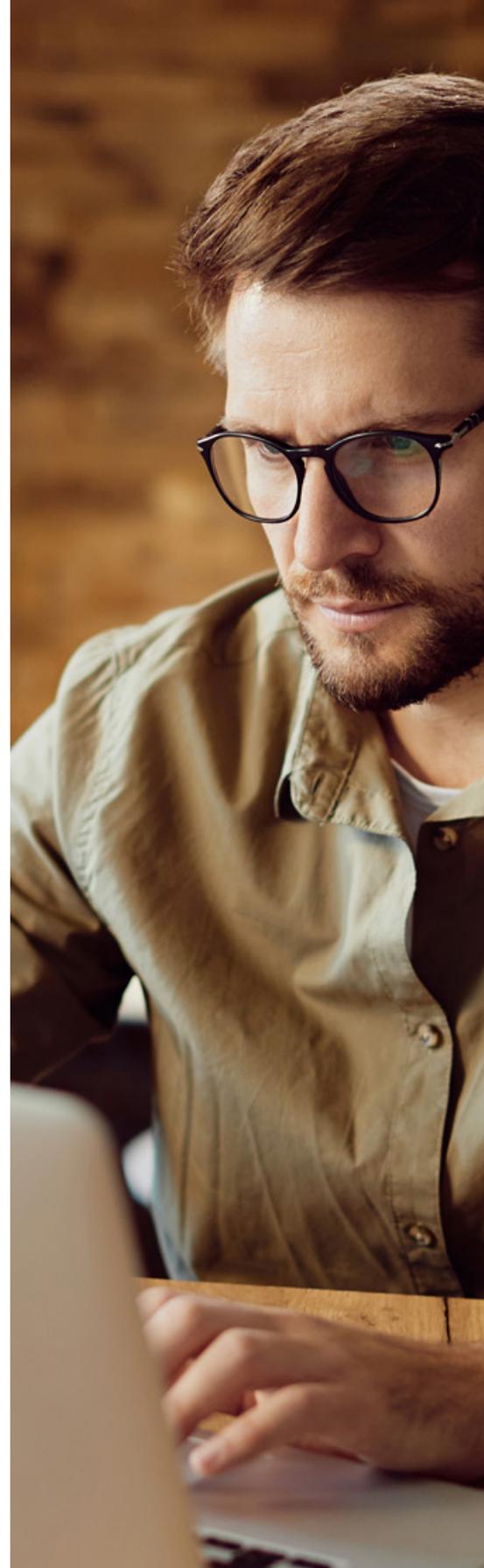
Ofertas gratuitas podem apresentar restrições de uso. Entre em contato com a Akamai para obter mais informações.

Advanced Security Management

O módulo opcional Advanced Security Management tem flexibilidade de automação e configuração para clientes com ambientes mais complexos de aplicações e necessidades avançadas de segurança. A opção Advanced Security Management inclui configurações adicionais de segurança, políticas de taxa, políticas de segurança, controles de DDoS na camada do aplicativo, regras de WAF personalizadas, segurança positiva de APIs e acesso à inteligência contra ameaças à reputação de IP (Client Reputation).

Managed Security Service

O suporte padrão é oferecido 24 horas por dia, 7 dias por semana, durante o ano todo para todos os clientes da Akamai. Além dos serviços profissionais sob demanda para consultoria ou trabalho em um único projeto, a Akamai fornece níveis de serviços gerenciados: serviço de WAAP totalmente gerenciado, suporte gerenciado contra ataques e suporte especializado a centros de operações de segurança.



Explore o App & API Protector e cadastre-se para fazer uma avaliação gratuita em akamai.com/aap