Akamai

WHITE PAPER

# Do WAF para a WAAP: a solução da Akamai para uma abordagem abrangente da segurança de aplicativos e APIs

# Índice

# Introdução

Com superfícies de ataque cada vez mais amplas e diversificadas, aumento do atrito e dos custos operacionais, além de ameaças multidimensionais altamente evasivas, as equipes de segurança necessitam de uma visibilidade que vá além dos firewalls tradicionais para proteger aplicativos da Web (WAF). Especificamente, eles precisam de mais ferramentas automatizadas para aumentar a eficiência e proteções mais detalhadas no ecossistema de apps e interfaces de programação de aplicativos (APIs). A terminologia mais moderna para essas proteções é proteção de APIs e aplicativos da Web (WAAP). Organizações criteriosas que priorizam a segurança de seus negócios e a proteção de seus clientes exigem uma proteção abrangente contra diversas ameaças em todo o seu ambiente digital.Além de proteger os aplicativos contra ataques conhecidos, desconhecidos e de dia zero, essas proteções incluem:

- Detecção adaptável contra ameaças
- Atualizações automatizadas de políticas
- Defesa robusta contra DDoS
- Descoberta e proteção de APIs
- Visibilidade e atenuação de bots
- Integrações fáceis para ciclos de vida de desenvolvimento

Este documento discute a tecnologia WAF tradicional, a mudança do WAF para a WAAP e a demanda constante do mercado que está desenvolvendo soluções WAAP. Como líder consolidada no setor de segurança, a Akamai concentra sua abordagem na inovação de tecnologias de segurança que movem e protegem a vida online dos usuários finais.

# Definição tradicional de um WAF

Um WAF tradicional fica no meio do fluxo de tráfego entre os usuários finais e um aplicativo da Web. O WAF monitora o tráfego HTTP, tanto criptografado quanto não criptografado, analisando e identificando possíveis ataques com base em um conjunto de regras predefinidas.

A maioria dos WAFs depende de uma lista predefinida de regras para identificar solicitações HTTP maliciosas misturadas ao tráfego legítimo, protegendo contra milhares de possíveis explorações conhecidas. Além disso, novos vetores de ataque e variações dos já existentes estão em constante evolução, sendo explorados por agentes mal-intencionados. É nesse ponto que um WAF tradicional precisa ser constantemente atualizado e ajustado para se adequar às características do tráfego legítimo, que variam conforme cada aplicativo e mudam ao longo do tempo.

Conforme os usuários finais passaram a exigir mais proteção e desempenho, os WAFs expandiram seu escopo para incluir tecnologias e serviços de segurança adjacentes, como atenuação de ataques de DDoS (negação de serviço distribuída), segurança de APIs e recursos de atenuação de bots. Essa evolução constante justifica uma nova definição e uma nova terminologia.

# Desafios de um WAF tradicional

Muitas organizações que utilizam WAF relatam que a solução não corresponde às expectativas iniciais em relação à eficácia, facilidade de gerenciamento e impacto nos aplicativos e APIs protegidos. Os WAFs frequentemente geram atritos dentro das organizações, impactam o desempenho e apresentam desafios na implantação devido aos protocolos de segurança. Isso ocorre porque a análise de bilhões de solicitações da web e de APIs em busca de código malicioso pode afetar o desempenho dos sistemas.

Alguns dos desafios de implementação mais significativos dos WAFs tradicionais decorrem do seguinte:

- Detecções imprecisas e altos índices de falsos positivos, criando fadiga de alerta e riscos adicionais
- WAFs dependem de análise, ajuste e manutenção manuais
- A falta de controles granulares leva a políticas de negação excessivamente rígidas, interrompendo a experiência do usuário final e os processos de negócios
- Inteligência desatualizada contra ameaças aumenta as vulnerabilidades
- Redução no desempenho e na cobertura, devido a restrições e inflexibilidade
- Muito limitados para proteger a expansão digital

WAFs tradicionais são uma ferramenta de segurança avançada. No entanto, muitas vezes podem deixar as organizações com problemas operacionais e riscos não atenuados, que serão abordados neste documento.

Organizações que pretendem atualizar sua tecnologia WAF com uma solução WAAP devem garantir que a solução ofereça valor comercial e proteções robustas de segurança. A conversão do WAF para a WAAP combina esse poder de proteção com funcionalidade, eficiência e facilidade de uso para atender às necessidades das empresas, tanto das equipes de segurança quanto de outras equipes.

# Princípios de design — WAF para WAAP

Como os WAFs tradicionais dependem da criação de regras pelo usuário final, qualquer fornecedor pode desenvolver e comercializar uma solução com relativa facilidade. Isso se evidencia na ampla oferta de produtos baseados no ModSecurity Core Rule Set, um conjunto de regras de código aberto do Open Worldwide Application Security Project (OWASP CRS).

No entanto, é difícil para um fornecedor projetar uma solução WAAP completa que possa:

- Ser implantada em linha para proteger aplicativos e APIs conforme surgem novas vulnerabilidades
- Acompanhar as práticas modernas de desenvolvimento de aplicativos
- Oferecer camadas igualmente fortes de defesa contra DDoS, atenuação de bots, proteção de API e proteções de aplicativos da Web no lado do cliente

Ao projetar nossa solução WAAP, a Akamai acreditava que deveria ir além do conceito de ser apenas "boa o bastante". O App & API Protector foi desenvolvido para enfrentar os riscos de segurança, permitindo que as organizações de nossos clientes mantenham o foco em seus principais objetivos empresariais. Como referência para nosso design, acreditamos que uma solução WAAP ideal deve proporcionar:

**Segurança eficaz**
Aplicativos estão envolvidos com todos os aspectos da empresa. Protegê-los contra ações maliciosas é o objetivo fundamental de uma equipe de segurança corporativa. Equipes de segurança têm o desafio de encontrar uma solução WAAP que ofereça as melhores detecções. A solução de segurança ideal deve priorizar a eficácia da detecção, sendo esse o aspecto mais crítico de um WAAP. Além disso, precisa demonstrar um histórico sólido na defesa contra ataques de dia zero, explorações e CVEs (Common Vulnerabilities and Exposures), além de manter uma alta disponibilidade.

**Precisão**
Equipes de segurança devem encontrar o equilíbrio certo entre atenuar riscos e permitir que a empresa se movimente com velocidade. Soluções ideais devem contar com mecanismos de autoajuste que minimizem falsos positivos, mas sem prejudicar a experiência do usuário final ou os processos de negócios.

**Proteções modernas**

Organizações precisam atualizar proteções de forma constante e muitas vezes manual, com base nas regras mais recentes para lidar com novas vulnerabilidades conforme aparecem. Para isso, precisam contar com duas capacidades fundamentais: acesso à inteligência mais atualizada sobre todos os vetores de ataque e especialistas em segurança que possam ajustar a estratégia de defesa para combater ameaças dinâmicas. A solução ideal será líder na comunidade de inteligência contra ameaças e fornecerá recursos que simplificam as operações de segurança em todas as proteções do patrimônio.

**Adaptabilidade**

O cenário das ameaças evolui rapidamente. Com a ameaça dos ataques impulsionados por IA, equipes de segurança precisam ser mais eficientes do que nunca em suas operações. As soluções WAAP ideais devem integrar automação avançada, aprendizado de máquina e inteligência global aprofundada para fornecer atualizações automáticas e recomendações personalizadas de modificação de regras, implementáveis com um único clique.

**Visibilidade**

Soluções tradicionais de WAF normalmente oferecem um fluxo interminável de alertas e dependem de profissionais de segurança para analisar cuidadosamente cada alerta emitido por recursos internos. Uma solução WAAP mais eficaz oferece visibilidade de várias soluções e contexto proativo para ataques, notificando uma organização quando, onde e como acontecem para aliviar a carga de recursos.

**Escalabilidade**

Uma solução sem escalabilidade suficiente para lidar com o tráfego de entrada pode facilmente se tornar um gargalo que aumenta a latência da Web e pode quebrar sob carga. Uma abordagem WAAP eficaz se ajusta de forma automática e contínua para atender às demandas de tráfego e atenuar ataques conforme evoluem, garantindo proteção ininterrupta sem comprometer o desempenho.

**Cooperação**
Uma solução de segurança eficaz deve ser integrável à estrutura atual, programável, fácil de usar e sem atritos. Uma solução ideal constrói uma ponte entre as equipes de segurança e desenvolvimento.

**Suporte**
Durante eventos de segurança desafiadores, as organizações muitas vezes ficam sobrecarregadas pela necessidade de habilidades e recursos para uma resolução ágil. Uma solução ideal deve oferecer tanto serviços gerenciados contínuos quanto opções sob demanda, garantindo expertise e atenuação para diversos cenários, como ataques em andamento, falhas de serviço, alta rotatividade de pessoal, lacunas de competências internas e outros desafios.

Com esses princípios de design em mente, vamos explorar como a Akamai aborda a criação da nossa solução WAAP líder, o App & API Protector, começando pela tecnologia principal. Nossa solução combina vários produtos de segurança em um só para enfrentar de forma holística os desafios de proteger aplicativos, defender-se contra ataques DDoS volumétricos, proteger APIs em todo o patrimônio e controlar o tráfego de bots.

# A abordagem da Akamai para a WAAP

## Ir além dos conjuntos de regras

Conforme o mercado evoluiu dos princípios tradicionais de design do WAF para a abordagem moderna e eficiente da WAAP, a tecnologia de detecção e atenuação permaneceu como prioridade.

A Akamai apresentou nosso WAF pela primeira vez em 2009 como o primeiro WAF baseado em edge do mundo. Na época, os fornecedores de segurança ofereciam WAFs baseados em conjuntos de regras estáticas como base para detecção de ameaças. Naquela ocasião, a Akamai se destacou ao criar o Kona Rule Set, um mecanismo proprietário baseado em regras que empregava um conjunto reduzido de regras flexíveis, em vez de estáticas, combinado a um modelo de pontuação de anomalias, proporcionando maior precisão e visibilidade sobre os ataques.

Então, em 2017, a Akamai introduziu grupos de ataque automatizados, eliminando a necessidade de as organizações configurarem e atualizarem constantemente as regras com as proteções gerenciadas pela Akamai. Os grupos de ataque automatizados representaram uma revolução, sendo rapidamente implementados em milhares de políticas ativas de WAF dos clientes da Akamai para aproveitar essa nova abordagem.

A Akamai continuou aprimorando sua abordagem à segurança de aplicativos, priorizando a proteção integrada de aplicativos e APIs, incluindo defesas contra bots. Com o lançamento do App & API Protector em 2021, essa solução WAAP foi projetada para substituir o Kona Site Defender WAF, atendendo empresas e negócios globais em expansão. O App & API Protector mudou a forma como a Akamai abordava as operações de segurança, modernizando a tecnologia Kona Rule Set no Adaptive Security Engine.

## Modernização das defesas contra DDoS na camada de aplicativo além da limitação de taxa

Quando se trata de DDoS, a limitação de taxa é uma ferramenta comprovada e eficaz. No entanto, o surgimento de ataques DDoS sofisticados na camada 7, investidas multivetoriais e a exploração de APIs deixaram as defesas tradicionais contra DDoS lutando para acompanhar. Defesas estáticas, que usam limites fixos e assinaturas predefinidas, são reativas e vulneráveis a falsos positivos, especialmente conforme os invasores passam a inserir tráfego mal-intencionado em solicitações legítimas. Foi aí que a Akamai mudou a abordagem da defesa contra DDoS e introduziu inovações, como a Proteção de URL e o Behavioral DDoS Engine.

O Behavioral DDoS Engine é uma adição de ponta ao App & API Protector da Akamai, que se junta ao Adaptive Security Engine como uma de suas principais tecnologias. Juntos, esses mecanismos oferecem uma proteção sem precedentes contra ameaças modernas, tornando a Akamai líder em WAAP. Essa abordagem de mecanismo duplo destaca a Akamai ao proporcionar atualizações automatizadas, ajuste autônomo e detecção contextual, garantindo uma experiência sem necessidade de intervenção manual.

## Solução única para uma proteção completa

Hoje, a segurança de aplicativos continua a ser redefinida por mudanças geradas pelas práticas modernas de desenvolvimento, como computação de edge sem servidor, arquiteturas baseadas em microsserviços, aplicativos de página única e modelos SaaS, IaaS, PaaS e FaaS. Isso acaba por influenciar a abordagem da proteção de aplicativos.

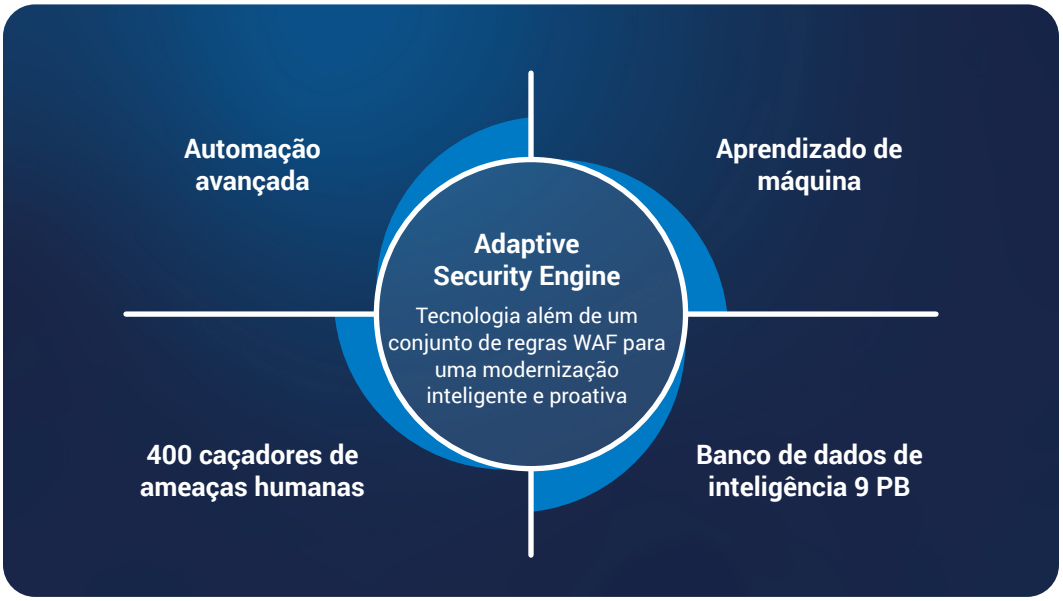
Para proteger aplicativos e APIs modernos em ambientes de TI complexos, a Akamai rearquitetou nossa tecnologia de segurança de aplicativos com uma abordagem mais adaptável, flexível e abrangente.  Conforme a solução WAAP da Akamai evoluiu do Web Application Protector e Kona Site Defender para o App & API Protector, mais recursos de segurança e conjuntos de ferramentas avançadas foram incorporados.

O App & API Protector agora oferece muitas melhorias adicionais de segurança, todas visíveis e controladas por apenas uma interface. A solução WAAP da Akamai combina:

1. O Adaptive Security Engine
2. Segurança de aplicativos com controles granulares
3. Defesa contra DDoS, incluindo proteção avançada contra DDoS da camada 7
4. Proteção de APIs, incluindo recursos de descoberta e proteção de informações pessoais identificáveis (PII).
5. Recursos de visibilidade e atenuação de bots
6. Uma plataforma com escalabilidade global, inteligência contra ameaças e resiliência

# O Adaptive Security Engine

O Adaptive Security Engine oferece proteção de última geração na interseção de aprendizado de máquina (ou ML, Machine Learning), inteligência de segurança em tempo real, especialistas em cibersegurança e automação avançada. Como tecnologia central da Akamai para detecção e defesa, o Adaptive Security Engine permite uma abordagem automatizada para proteger aplicativos da web e todo o ecossistema de APIs. A solução também fortalece a evolução da Akamai do WAF para a WAAP, integrando soluções de segurança correlacionadas, como gerenciamento de bots, proteção contra DDoS, integrações com DevOps, entre outras.




O Adaptive Security Engine é único porque aprende os padrões de tráfego e ataque exclusivos de cada cliente, analisa as características de cada solicitação em tempo real e usa esse conhecimento para interceptar e se adaptar a ameaças futuras. A solução usa o mesmo insight e inteligência da plataforma para reduzir os falsos positivos por meio de recomendações de ajuste. Esse recurso de autoajuste oferece facilidade de uso pelas equipes de segurança e desenvolvimento, proporcionando proteções adaptáveis, como atualizações proativas, contra ameaças.

## Detecção adaptável contra ameaças

O mecanismo emprega um modelo multidimensional de pontuação de ameaças que combina a inteligência da plataforma com dados/metadados de cada solicitação. Esses dados são acionados com lógica de tomada de decisão para identificar ataques reais com precisão.

Detecções adaptativas são especialmente eficazes na identificação de ataques altamente direcionados, evasivos e furtivos, pois atacantes sofisticados investem mais tempo e esforço em seus ataques. Conforme os invasores exploram vulnerabilidades e configurações incorretas, o Adaptive Security Engine coleta e correlaciona evidências sobre suas táticas, aumentando a capacidade de identificar um histórico de ataques.

Além da carga útil real e de seu local na solicitação, outros exemplos de dimensões de ataque avaliados para cada cliente incluem:

- Um histórico de reconhecimento e/ou ataques (por exemplo, frequência, magnitude, gravidade)
- Qualquer sinal de automação mal-intencionada e ferramentas de ataque
- Correlação com fontes conhecidas de tráfego de ataque

Além disso, o Adaptive Security Engine é aprimorado com duas tecnologias exclusivas: Smart Detect, que tokeniza a entrada em uma impressão digital para uma detecção altamente precisa, e Smart Sniff, que identifica corretamente o tipo de conteúdo do corpo da solicitação para evitar manipulação de conteúdo e tentativas de evasão. Pesquisadores de ameaças da Akamai usam a ampla infraestrutura e os sistemas da Akamai para executar passivamente novas detecções em todo o tráfego de produção e, em seguida, analisar esses resultados usando modelos de ML.

## Atualizações automáticas

Atualmente, muitas organizações não possuem os recursos ou o conhecimento necessário para monitorar continuamente ameaças emergentes, atualizar configurações e reavaliar o tráfego da web para otimizar suas políticas de segurança. Para enfrentar esse desafio, a Akamai atualiza continuamente o Adaptive Security Engine por meio de uma estrutura de testes automatizados baseada em IA/ML, garantindo alta precisão diante das ameaças em constante evolução. Essas atualizações frequentemente oferecem proteção contra ataques de dia zero antes mesmo de sua divulgação.

## Estrutura de testes para garantir a precisão

O teste de uma solução WAAP se baseia em uma premissa simples: testar diferentes vetores de ataque e bloquear ataques da Web. Entretanto, é preciso ser considerado o seguinte:

- Ambientes do mundo real são mais complexos do que ambientes de teste e muitas vezes levam a falsos positivos e falsos negativos.
- Projetar uma estrutura de testes com precisão requer não apenas uma verificação adicional da detecção de ataques, mas fazer isso sem acionar falsos positivos ou falsos negativos por acidente.
- O teste requer o uso de tráfego real na Web, tanto legítimo quanto de tráfego de ataque.

As atualizações do Adaptive Security Engine consistem em vários estágios para garantir que o tráfego legítimo não seja afetado negativamente:

- Todas as detecções são testadas em laboratório com o uso de tráfego sintético para garantir que detectem adequadamente os ataques e não introduzam falsos positivos.
- As atualizações são, então, testadas no tráfego produzido ao vivo, a fim de garantir que a amostra seja válida para o tráfego atual da plataforma. Esse processo envolve que a atualização seja feita em modo sombra no tráfego real do cliente. O modo sombra garante que o tráfego do cliente não seja afetado e que o teste de detecção continue acontecendo com precisão.
- Depois que uma atualização passa pelo segundo estágio, o ML identifica padrões ou acionadores que a análise humana pode ter deixado passar, após o que a Equipe de pesquisa de ameaças analisa manualmente os resultados.
- Somente quando essas verificações são aprovadas em cada fase é que uma alteração pode passar para a próxima fase e ser implantada em um segmento maior da rede. Após 100% de implementação, os recursos de autoajuste eliminarão quaisquer falsos positivos remanescentes específicos dos padrões de tráfego dos clientes.

## Autoajuste automático

O autoajuste automático alivia o ônus do ajuste manual, que pode levar a políticas desatualizadas e a erros humanos, e cria uma experiência quase sem intervenção humana. O Adaptive Security Engine aplica ML, modelos estatísticos e heurística em todos os acionadores de cada política de segurança para diferenciar com precisão entre ataques reais e tráfego de usuário final identificado erroneamente como ataques. Não se trata de uma verificação genérica em toda a plataforma aplicada apenas durante a integração, mas de um processo de ajuste constante realizado 24 horas por dia, 7 dias por semana, durante o ano todo, sem configuração ou intervenção do usuário final.

O autoajuste é simples e sem atrito. Administradores de segurança podem facilmente examinar e aceitar as recomendações com um clique por meio da interface do usuário ou podem automatizar usando APIs AppSec, a interface de linha de comando (CLI) ou o Terraform. Para maior transparência, um link pré-filtrado para o Web Security Analytics mostra todas as solicitações consideradas como falsos positivos com uma justificativa fornecida para cada recomendação de ajuste.

## Flexibilidade de configuração e automação

Quando um fornecedor de soluções WAAP ultrapassa a tecnologia tradicional de conjunto de regras, a configuração e a automação ficam mais flexíveis. O Adaptive Security Engine permite:

- Disponibilizar diferentes tipos de atualizações para o WAF (automáticas ou manuais) conforme as necessidades de cada aplicativo e seu nível de tolerância ao risco
- Controlar ações por grupo de ataque e regra contributiva, garantindo a personalização quando o comportamento do aplicativo ou do tráfego não for padrão
- Configurar condições simples e complexas para diferentes características de solicitação, como IP, geolocalização, cabeçalho, carga útil, entre outras
- Reduzir proativamente as fontes de ameaças que foram detectadas realizando ataques/varreduras suspeitas de WAF para seus próprios aplicativos, com o Penalty Box
- Modificar o cabeçalho de depuração
- Modificar as configurações de tamanho de inspeção de carga útil de solicitação ou de registro de carga útil de ataque
- Fazer simulações de mudanças na lógica de detecção para colocar essas mudanças em produção com confiança

## Verificação no mundo real

O modo de avaliação oferece aos clientes da Akamai flexibilidade e granularidade na configuração de versões específicas do Adaptive Security Engine e no teste de atualizações ou novas regras/políticas. Clientes podem ver as novas atualizações ou alterações antes de optar por ativá-las, conforme adequado ou necessário para seu ambiente específico de aplicativos da Web. Para uma modernização eficaz da segurança, a Akamai acredita que os testes em tráfego em tempo real melhoram os resultados de segurança em relação aos testes em tráfego passado. O modo de avaliação é semelhante à aplicação de uma regra sombra, em que é possível ver os resultados em tempo real como se a política fosse aplicada, mas sem impacto para os usuários finais atuais. Organizações podem optar por esse modo de operação manual/avaliação para minimizar o impacto inesperado sobre falsos positivos e falsos negativos.

## Integração de proteções modernizadas

As equipes de segurança e DevOps também podem operacionalizar a segurança integrando chamadas às APIs da Akamai usando a CLI, o Akamai Terraform ou scripts em seu pipeline de automação de CI/CD. A flexibilidade de configuração e automação garante que a segurança avançada nunca atrapalhe a velocidade de desenvolvimento. Essas integrações podem:

- Permitir uma rápida integração de aplicativos
- Permitir o gerenciamento uniforme de políticas de segurança em grandes portfólios de aplicativos
- Centralizar a aplicação da segurança em infraestruturas híbridas e multinuvem
- Melhorar a colaboração entre as equipes de DevOps e de segurança em um fluxo de trabalho GitOps para obter uma cobertura ideal

Além disso, o gerenciamento de eventos e informações de segurança (SIEM) permite coletar eventos de segurança que ocorrem na plataforma da Akamai. Por sua vez, nossa solução de integração de SIEM fornece uma maneira de entregar eventos de SIEM para ferramentas analíticas de SIEM locais e baseadas em nuvem, como Splunk e QRadar, para que você possa incorporar os eventos de segurança da Akamai em sua infraestrutura geral de eventos e segurança em quatro etapas básicas.

Você pode proteger e controlar seu feed de dados com:

- **Filtragem de eventos**
  Use a configuração e a política de segurança para ajudar você a se concentrar nas ameaças reais.
- **Retenção de dados**
  O coletor armazena dados por 12 horas para que seja possível capturar eventos perdidos.
- **Proteção contra sobrecarga de SIEM**
  É possível definir em seu conector SIEM um número máximo de eventos de segurança obtidos em cada solicitação. Isso ajuda a evitar a sobrecarga do aplicativo SIEM.
- **Intervalo de busca**
  É possível definir a frequência com que os conectores SIEM fazem uma chamada para a API do SIEM para obter dados de eventos de segurança.

# Segurança de aplicativos e defesa contra DDoS

A segurança de aplicativos é um aspecto crucial da cibersegurança moderna, garantindo que os aplicativos permaneçam resilientes contra uma grande variedade de ameaças e vulnerabilidades. Sua importância está em várias áreas fundamentais. Integridade e confidencialidade dos dados são fundamentais, pois a segurança dos aplicativos garante que os dados confidenciais sejam protegidos contra acesso não autorizado e adulteração. Ela também desempenha um papel fundamental na continuidade dos negócios, protegendo os aplicativos contra interrupções causadas por incidentes de segurança, garantindo, assim, uma disponibilidade constante dos serviços. Além disso, a segurança de aplicativos é essencial para o gerenciamento da reputação, evitando violações que podem prejudicar a reputação de uma organização e minar a confiança do cliente. Por fim, isso ajuda as organizações a cumprir os requisitos regulamentares, evitando penalidades legais e financeiras.

Como função, uma solução WAAP filtra e monitora o tráfego HTTP entre aplicativos da Web e a Internet. Isso protege contra ataques comuns baseados na Web, como XSS, injeção de SQL e DDoS.

O App & API Protector é reconhecido por sua proteção contra DDoS líder de mercado, projetada para combater ataques volumétricos destinados a sobrecarregar os recursos. A solução combate o DDoS das seguintes maneiras:

- **Atenuação de DDoS baseada em edge**
  Ao usar a plataforma de edge distribuída globalmente da Akamai, o App & API Protector pode eliminar instantaneamente os ataques DDoS antes que eles atinjam a origem do aplicativo. Essa abordagem edge-first garante latência mínima e proteção máxima sem afetar o desempenho do aplicativo.

- **Limitação da taxa**
  O App & API Protector inclui limitação de taxa adaptável para defender-se contra ataques DDoS na camada de aplicativos distribuídos. Esses controles podem ser configurados para limitar a taxa de solicitações recebidas com base em vários critérios, incluindo, entre outros, IP, localização geográfica, controles de reputação de IP, vários cabeçalhos HTTP e condições de correspondência.

- **Proteção de URL com eliminação inteligente**
  Adota uma abordagem diferente para a limitação de taxas. Com o URL Protection, é possível proteger sua origem contra solicitações excessivas com base na taxa de solicitação aceitável (RPS máximo), dependendo da capacidade da origem. A solução foi concebida especificamente para proteger URLs com muita computação, endpoints de API etc. contra ataques DDoS de camada de aplicativos altamente distribuídos.

- **Behavioral DDoS Engine**
  Novo no App & API Protector, o Behavioral DDoS Engine é uma ferramenta avançada para uma estratégia de defesa em profundidade. A solução adota uma abordagem eficiente para o gerenciamento e a atenuação de eventos DDoS, utilizando aprendizado de máquina para definir padrões de tráfego e detectar anomalias em relação ao comportamento esperado. O mecanismo opera analisando as variações nos padrões de tráfego, permitindo que os usuários configurem a resposta do sistema a diferentes anomalias sem a necessidade de definir limites explícitos, o que reduz a carga operacional de gerenciamento e ajustes.

- **Atualizações automáticas e autoajuste**
  Com o uso da estratégia de dois mecanismos da Akamai, o Adaptive Security Engine e o Behavioral DDoS Engine, o App & API Protector se adapta constantemente às novas ameaças com atualizações automáticas e autoajuste orientado por ML, a fim de reduzir a carga operacional.

## Behavioral DDoS Engine: como funciona

No centro do Behavioral DDoS Engine está um modelo avançado de ML que monitora constantemente o tráfego em tempo real, estabelecendo linhas de base para o comportamento normal e detectando instantaneamente os desvios que indicam um ataque. Ao analisar os padrões de tráfego em várias dimensões dinâmicas, como país de origem, padrões de TLS, IP e impressões digitais de TLS, esse mecanismo pode identificar rapidamente anomalias e agir.

Os principais componentes do Behavioral DDoS Engine incluem:

- **Monitoramento de comportamento em tempo real**
  O mecanismo analisa constantemente o tráfego e estabelece linhas de base da atividade normal, detectando instantaneamente os desvios que sinalizam possíveis ataques DDoS.

- **Aprendizado de máquina para precisão**
  Modelos avançados de aprendizado de máquina, ou ML (Machine Learning), potencializam a capacidade do mecanismo de identificar anomalias sutis nos padrões de tráfego, garantindo uma atenuação precisa sem bloquear usuários legítimos.

- **Atenuação proativa**
  Usando insights da rede global da Akamai (1.056 TB de tráfego por dia), o mecanismo prevê e neutraliza ataques, muitas vezes antes que possam afetar as empresas.

- **Análise multidimensional**
  O tráfego é avaliado em várias dimensões, incluindo padrões de IP, país e TLS, proporcionando uma proteção robusta e adaptada às necessidades de cada aplicativo

**Arquitetura avançada para uma defesa superior**
O Behavioral DDoS Engine opera por meio de uma arquitetura sofisticada que inclui vários componentes essenciais:

- **Mecanismo de detecção**
  Usa dimensões dinâmicas e dados históricos de ataques para identificar ataques DDoS em tempo real.
- **Mecanismo de atenuação**
  Implementa contra-ataques automáticos, usando inteligência do gerador de linha de base e sinais de ameaça para reduzir a sobrecarga operacional das equipes de segurança.
- **Redução de ruído/falso positivo**
  Modelos de ML filtram dados irrelevantes, garantindo que o tráfego limpo seja usado para análise e atenuação.
- **Gerador de parâmetros**
  Refina continuamente os perfis de tráfego ao processar dados limpos por um período de duas semanas, permitindo que o mecanismo se mantenha atualizado em relação às estratégias de ataque mais recentes.
- **Validador de parâmetros**
  Com a ajuda da IA, esse componente crucial avalia centenas de ataques DDoS todos os meses para aperfeiçoar a solução.

Essa estrutura automatizada garante que as equipes de segurança possam contar com o mecanismo para um ajuste dinâmico das defesas, sem intervenção manual. A solução detecta e filtra atividades anormais de tráfego, como tráfego gerado por bots ou tentativas de DDoS, protegendo aplicativos de forma eficaz.

## Precisão na segurança de aplicativos

Uma solução de segurança de aplicativos (WAF ou WAAP) que não seja precisa exige mais recursos internos para gerenciar o aumento do número de alertas diários. Imprecisões podem gerar um grande número de falsos positivos (quando uma solicitação é sinalizada como maliciosa, mas não é) e falsos negativos (quando uma solicitação é sinalizada como não maliciosa, mas é), desperdiçando valiosos conjuntos de habilidades de segurança e tempo na pesquisa e análise desses tipos de alertas.

Organizações geralmente enfrentam o desafio da fadiga de alertas, mas permanecem sem uma solução devido a controles ou recursos muito amplos que corrigem demais ou de menos. Isso geralmente leva a organização a colocar o WAF em off-line ou, pior ainda, a ignorar os alertas e as atualizações de versão. Embora isso alivie muitas preocupações organizacionais sobre o bloqueio acidental de usuários legítimos, também protege menos contra ataques a APIs via Web. Muitas organizações também não têm a granularidade dos controles para equilibrar o acesso ao tráfego legítimo e bloquear o tráfego mal-intencionado com precisão.

A vantagem de uma solução WAAP eficaz é reduzir tanto os falsos positivos quanto os falsos negativos, usando um conjunto completo de controles e recursos WAAP para aumentar a precisão e minimizar o impacto sobre usuários legítimos.

### Compreensão da precisão

Precisão é a medida da capacidade de um WAF ou WAAP para interromper simultaneamente os ataques sem bloquear usuários legítimos. A precisão considera quatro variáveis:

- **Positivos verdadeiros (PV):** ataques reais identificados corretamente como mal-intencionados
- **Falsos positivos (FP):** solicitações legítimas identificadas incorretamente como mal-intencionadas
- **Verdadeiros negativos (VN):** solicitações legítimas passadas para o aplicativo
- **Falsos negativos (FN):** ataques reais indevidamente passados para o aplicativo

## Classificações do Client Reputation

Client Reputation é uma solução que usa um mecanismo sofisticado de análise de risco para calcular um conjunto de "pontuações de risco" para cada endereço IP que tenta acessar seu site. A solução analisa endereços IP de entrada e usa vários fatores, como persistência do invasor, número de aplicativos visados, gravidade do ataque, magnitude, setor e ataques anteriores direcionados aos aplicativos de um cliente para determinar uma pontuação que especifica a probabilidade de esse endereço IP se envolver em um ataque via Web, inclusive:

- **DOSATCK**
  Usa botnets para lançar ataques de negação de serviço (DoS). O objetivo de um ataque DoS é inundar um site com solicitações falsas, para que o site fique extremamente lento ou até mesmo seja derrubado. Em um ataque de negação de serviço distribuída (DDoS), essas solicitações vêm de milhares de locais (geralmente computadores ou telefones infectados por malware), o que torna impossível interromper o ataque simplesmente bloqueando um determinado endereço IP.

- **SCANTL**
  Ferramentas de varredura podem identificar possíveis riscos à segurança, como injeção de SQL, falsificação de solicitações entre websites (CSRF), redirecionamentos inválidos e outras vulnerabilidades. Executar uma ferramenta de varredura da Web em seu próprio site é uma boa ideia. O que não é nada bom é ter um agente mal-intencionado rodando uma ferramenta de varredura em seu site.

- **WEBATCK**
  Usa técnicas como injeção de SQL, inclusão remota de arquivos ou cross-site scripting para fazer coisas como instalar malware ou roubar dados do usuário. Um hacker pode conseguir recuperar todos os seus dados de usuário, inclusive senhas, números de cartão de crédito e de identidade e qualquer outra informação que possa ter sido armazenada no banco de dados do usuário.

- **WEBSCRP**
  Usa ferramentas automatizadas para baixar uma cópia de uma página da Web e "raspar" (ou seja, copiar) todo o conteúdo dessa página. O conteúdo pode ser reaproveitado para usos ilegais ou antiéticos.

Com o Client Reputation, é possível proteger a organização de forma proativa contra fontes suspeitas de ameaças com base na inteligência cumulativa de ameaças do Akamai Connected Cloud.

# Proteção contra malware

Agentes de ameaças usam malware como tática comum de ataque. A Akamai tem uma solução completa para proteção de aplicativos. Organizações de todos os tamanhos permitem uploads de arquivos para aumentar a eficiência interna e externa, incluindo esses usos comuns:

- Currículos para candidaturas a empregos
- Contratos de trabalho, integração, E-Verify, configuração de depósito direto e outros
- Solicitações, incluindo empréstimos, configuração de contas e solicitações de crédito
- Estimativas de seguros ou reparos de automóveis, residências e outros
- Prontuários médicos para seguro ou configuração de conta de paciente
- Avaliações de produtos ou experiências de clientes que incluem imagens

A proteção contra malware na segurança de aplicativos e APIs detecta e isola ameaças de malware na edge antes que atinjam o sistema corporativo visado. Organizações podem proteger tempo, orçamento e produtividade, bem como dados internos e dos clientes, com os benefícios da proteção contra malware para aplicativos e APIs:

- **Detecte e bloqueie malware na edge**
  Evite os riscos da varredura em servidores, onde o malware já pode ter se espalhado no momento da varredura.
- **Evite a complexidade e ganhe tempo**
  Faça a varredura de arquivos apenas uma vez, em vez de configurar a proteção em cada sistema, como acontece com scanners ICAP e baseados em agentes.
- **Posicione a postura de segurança para o crescimento**
  Ao escolher uma abordagem preventiva e em camadas, as organizações podem escalonar sua proteção conforme os negócios crescem, oferecendo proteção adicional na edge e a opção de nova varredura na origem.
- **Forneça consistência aos aplicativos**
  As empresas não precisam configurar ou alterar o código do aplicativo.
  A proteção contra malware fica completamente hospedada na Akamai Connected Cloud.

# Análise de segurança de aplicativos

O App & API Protector traz incluído o produto mais amado (e mais usado) da Akamai: o Web Security Analytics. Essa solução WAAP da Akamai permite capturar eventos de segurança que ocorrem no aplicativo da Web e nas APIs na plataforma da Akamai, para visualização nas ferramentas de análise de segurança disponibilizadas.

O Web Security Analytics é um componente vital da cibersegurança moderna, oferecendo insights completos sobre o tráfego da Web e possíveis ameaças. Ao analisar uma grande variedade de pontos de dados, incluindo padrões de tráfego, comportamento do usuário e eventos de segurança, a solução permite uma visibilidade detalhada da postura de segurança dos aplicativos na Web. Essa abordagem proativa permite que organizações detectem e respondam a ameaças com mais eficiência, reduzindo riscos antes que possam causar danos significativos. O Web Security Analytics não apenas ajuda a identificar atividades mal-intencionadas, como ataques de bots, injeções de SQL e cross-site scripting, como auxilia na compreensão e no tratamento de vulnerabilidades dos aplicativos na Web. Além disso, respalda esforços de conformidade, gerando relatórios que demonstram a adesão a políticas de segurança e requisitos regulamentares.

# Descoberta e criação de perfil de API

As APIs permitem que organizações criem experiências avançadas na Web e em dispositivos móveis, geralmente expondo dados e lógica de back-end para desenvolver ofertas novas e inovadoras. As APIs também expandem a superfície de ataque. As organizações precisam entender quais endpoints de API estão em seu ambiente, as funções da API e os perfis de tráfego. O recurso de descoberta e criação de perfil de API da Akamai faz exatamente isso e muito mais, de forma automática e constante.

O recurso de descoberta de API alerta as equipes de segurança sobre novos aplicativos e APIs, muitas vezes desprotegidos, que estão conectados por diferentes linhas de negócios em uma organização. Essa tecnologia de detecção automatizada é um novo recurso da solução WAAP da Akamai para manter as equipes de desenvolvimento, os líderes de linha de negócios e as equipes de segurança alinhados.

O Adaptive Security Engine descobre automaticamente as APIs a cada 24 horas, com base em um mecanismo de pontuação que leva em conta o tipo de conteúdo da resposta, as características do caminho e os padrões de tráfego. Os dados de descoberta incluem informações sobre a especificação da API observada com detalhes como:

- Nome do host
- Caminho base
- Caminho do recurso
- Parâmetros e seus tipos de dados
- Métodos
- Formato da API

Caminhos base e de recursos são determinados conforme um algoritmo que leva em conta a profundidade do caminho, a contagem de descendentes e os similares do tráfego observado em um nome de host específico com tráfego de API. No caminho do recurso, se um parâmetro for observado para um método específico, ele será marcado e o tipo de dados desse parâmetro será identificado.

O perfil de tráfego para os pontos de extremidade da API contém informações que oferecem insights sobre o objetivo da API e o nível de ameaça atual. Alguns dos pontos de dados incluídos são:

- Total de solicitações desde que a API foi descoberta pela primeira vez, tanto nas últimas 24 horas quanto na tendência ao longo do tempo
- Data em que a API foi descoberta pela primeira vez e vista pela última vez
- Número de solicitações entre diferentes métodos, como GET, PUT, POST, DELETE e OPTIONS
- Número de solicitações que geram 2xx, 3xx, 4xx e 5xx respostas
- Identificação do cliente final com base no agente de usuário
- Erros de resposta, como a porcentagem de tráfego que resulta em erros no lado do cliente e no lado do servidor
- Ocorrências de agentes de ameaças conhecidos, incluindo a porcentagem do tráfego total proveniente de agentes mal-intencionados conhecidos da plataforma Akamai, dividido por invasores da Web, scanners da Web, scrapers e invasores DoS

Proteger APIs pode ser um obstáculo significativo sem visibilidade. Como uma organização protege o que não pode ver? Com a Akamai, as empresas podem descobrir e definir perfis de APIs de maneira automática e contínua, incluindo seus pontos de extremidade, definições e caraterísticas de recursos e tráfego. Assim que as APIs são identificadas, a Akamai oferece ampla proteção para lidar com DoS, injeção mal-intencionada, ataques de abuso de credenciais e violações de especificações de APIs. A abordagem independente de nuvem e origem da Akamai permite fácil descoberta de APIs em todo o estado do aplicativo sem qualquer configuração adicional exigida pelo usuário final. Essa visibilidade permite que desenvolvedores, proprietários de aplicativos e equipes de segurança pensem à frente de APIs novas, desconhecidas ou em constante mudança e as registrem facilmente para proteção.

# Visibilidade e atenuação de bots

Como bots são responsáveis por mais da metade do tráfego de um website, pode ser difícil saber quais bots estão ajudando sua organização a atingir metas e quais têm a intenção de prejudicar. Bots úteis criam eficiências na organização automatizando avaliações, conversas ou recomendações. Bots mal-intencionados podem obstruir os caminhos do tráfego e afetar a experiência operacional e do cliente, afetando a receita. No App & API Protector, a visibilidade e atenuação de bots permitem detecções avançadas de bots úteis para deixá-los passar, enquanto bloqueiam bots prejudiciais. Isso permite que a organização:

- **Veja os bots e entenda seu impacto**
  Visibilidade de tráfego de bots é essencial para empresas digitais modernas, considerando-se o uso generalizado de bots para operações como pesquisa, verificação do desempenho do site e interação com parceiros de negócios.
- **Melhore o controle operacional**
  O bloqueio de bots mal-intencionados permite maior eficiência, reduz os riscos comerciais e financeiros e controla melhor os gastos com TI.
- **Tome decisões melhores baseadas em dados**
  Análises e relatórios detalhados ajudam você a fazer escolhas criativas e eficazes sobre as jornadas dos clientes, a postura de segurança, a tolerância a riscos e as operações de TI.

## Visibilidade e atenuação de bots intrínsecas ao App & API Protector

O App & API Protector oferece detecções e controles de tráfego de bots que podem afetar de forma adversa o desempenho e a segurança das propriedades na Web. A solução oferece visibilidade antecipada para um monitoramento proativo de anomalias e ameaças envolvendo bots ao longo do tempo.

Com o uso da solução de bot da Akamai no App & API Protector:

- Acesse mais de 1.700 bots definidos conhecidos pela Akamai
- Tenha visibilidade do tráfego de bots em tempo real
- Crie definições de bots personalizadas
- Permita bots úteis e recuse bots ruins
- Tenha visibilidade de bots e relatórios de tendências

Para websites com problemas avançados de bots, a Akamai oferece o Bot Manager, que traz proteções avançadas contra bots para aumentar o comércio eletrônico e a segurança digital. O Bot Manager oferece ações mais diferenciadas para bots persistentes e adversos, em casos, por exemplo de ataques como:

- Preenchimento de credencial
- Acúmulo de inventário
- Captura de conteúdo e de preços
- Violação de lógica de negócios

## Principais recursos de bot

A Akamai reconhece a evolução das necessidades de gerenciamento de bots via WAAP. Assim, elevamos nossas ferramentas de visibilidade e atenuação de bots para incluir recursos recém-incorporados, como:

- **Detecção de personificação por navegador**
  Esse favorito dos clientes do Akamai Bot Manager usa modelos de pontuação dinâmicos e ML para discernir e neutralizar as atividades de bots no navegador, e está incluído no App & API Protector.
- **Ações de resposta condicional**
  Os clientes agora têm uma compreensão melhor das atividades de bots no navegador e podem responder com ações condicionais para aplicar diferentes estratégias de resposta contra bots mal-intencionados.
- **Ações desafiadoras**
  Faça com que os bots enfrentem uma série de ações de desafio diferentes, incluindo desafios intersticiais que, quando não resolvidos, permitem bloquear o acesso ao conteúdo.

# Mais do que um WAF: benefícios da solução Akamai

A abordagem da Akamai para a WAAP resultou na solução App & API Protector. No entanto, não é só um produto que beneficia nossos clientes WAAP. Criado com base na plataforma global mais distribuída e com a tecnologia de centenas de especialistas em ameaças humanas, o Akamai Connected Cloud oferece desempenho, disponibilidade, inteligência, experiência e resultados de segurança eficazes.

# Inteligência e detecção de ameaças

Ter um recurso robusto e interno de inteligência contra ameaças melhora a capacidade do fornecedor de WAAP para responder a ameaças em evolução. No entanto, são a qualidade, a pontualidade e a capacidade de ação da inteligência fornecida que determinarão o grau de impacto sobre a eficácia da segurança dos aplicativos. A Akamai usa o Akamai Connected Cloud para analisar constantemente os dados disponíveis e identificar tendências atuais no cenário de ameaças, novos vetores de ataque quando detectados pela primeira vez e invasores ativos no momento. Em seguida, a Akamai incorpora essa inteligência à nossa solução WAAP de várias maneiras.

O Adaptive Security Engine da Akamai, apresentado anteriormente neste documento, combina dois níveis de inteligência avançada contra ameaças para criar um mecanismo poderoso e exclusivo, a fim de gerenciar automaticamente as proteções mais recentes de nossos clientes. Além do ML e da adoção de regras automatizadas, o Adaptive Security Engine apresenta inteligência contra ameaças da plataforma global da Akamai e uma grande equipe de pesquisadores especializados em ameaças.

## Inteligência da plataforma Akamai

Com uma das maiores plataformas globais, a Akamai consegue analisar o tráfego de ataques em escala global, garantindo proteção rápida e eficiente para todos os seus clientes. Nossa base de dados de inteligência inclui, em média, 1.056 TB de dados de ataques por dia. Ela aproveita a visibilidade da Akamai sobre o tráfego da web em milhares dos maiores, mais acessados e mais frequentemente atacados negócios online para obter dados relevantes e de alta qualidade, que são analisados pela Equipe de Pesquisa de Ameaças da Akamai:

- **Gatilhos WAAP**
  Ingere dados diretamente das implantações WAAP globais da Akamai, capturando eventos de ataque reais direcionados a todos os clientes de segurança da Akamai.

- **Registros de CDN (Rede de Entrega de Conteúdo)**
  Incorpora a análise offline realizada em registros de eventos de todos os clientes da Akamai, incluindo aqueles que não implantaram sua solução WAAP.

A base de dados de inteligência da Akamai abriga um dos maiores conjuntos de dados do mundo (9 PB). Para as organizações que priorizam a segurança dos negócios e dos clientes, a inteligência contra ameaças da Akamai lidera os provedores de soluções WAAP.

## Pesquisa sobre ameaças e resposta a incidentes

Organizações de pesquisa sobre ameaças e resposta a incidentes fornecem inteligência e análise humanas para complementar e ampliar a cobertura de ataques de uma solução WAAP. A Akamai emprega várias equipes com diferentes atribuições para dar suporte aos nossos clientes WAAP, bem como identificar novos vetores de ataque que podem exigir proteções adicionais.

### Pesquisas sobre ameaças

A equipe de pesquisas sobre ameaças da Akamai realiza análises regulares das tendências de ataques na Web em toda a base de clientes da Akamai, bem como análises personalizadas para clientes individuais, conforme necessário. A equipe também projeta e implementa heurísticas para consultar inteligência prática para dar suporte à criação e às atualizações da lógica de regras principais do WAF e da Client Reputation.

### Resposta a incidentes

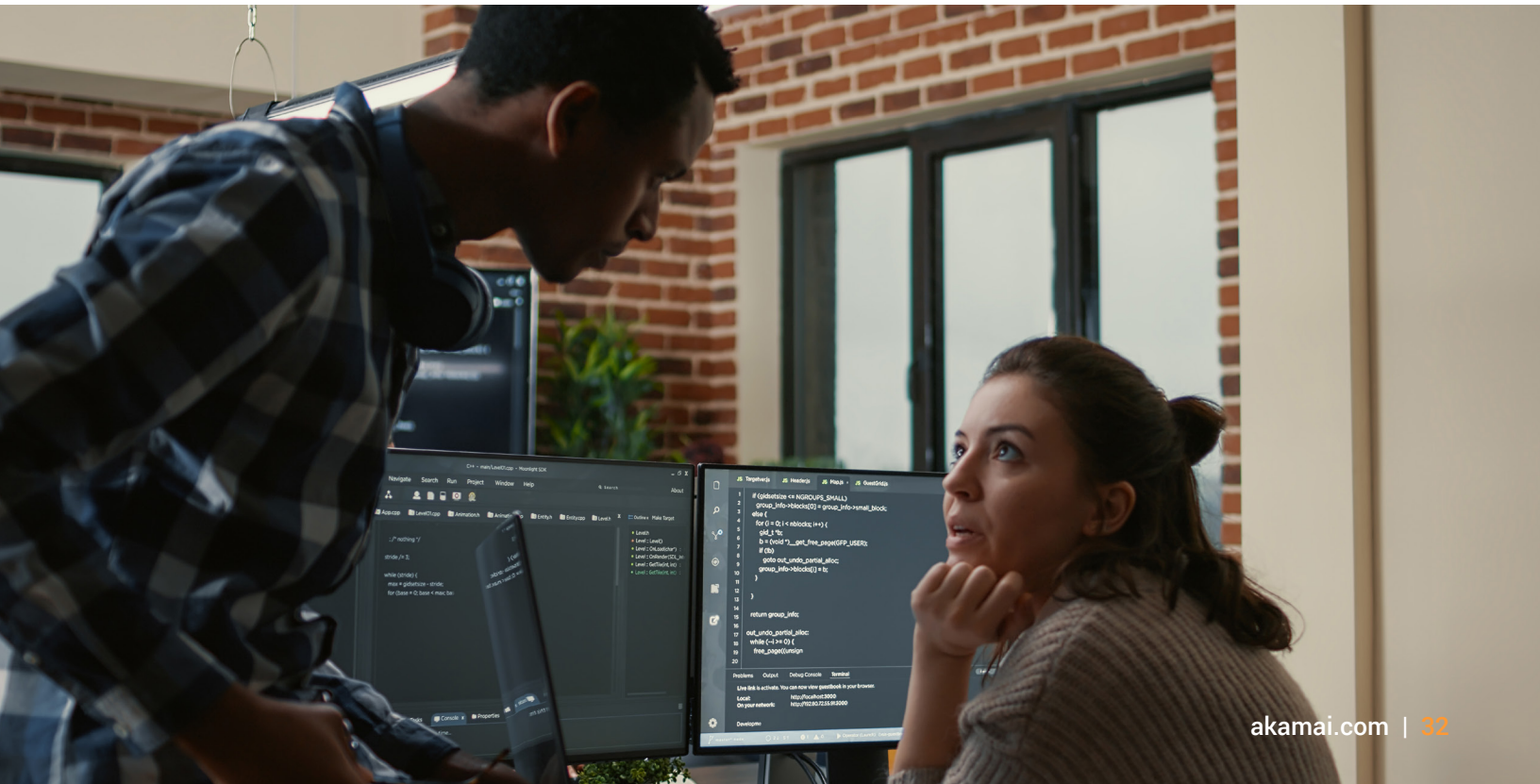
A Akamai opera duas equipes de resposta a incidentes, a CSIRT (Computer Security Incident Response Team, equipe de resposta a incidentes de segurança de computadores) e a SIRT (Security Intelligence Response Team, equipe de resposta a incidentes de inteligência de segurança), para trabalhar com o SOC (Security Operations Center, centro de operações de segurança) global da Akamai e fornecer análise e resposta a incidentes para clientes individuais quando eles sofrem um ataque. Além disso, a CSIRT monitora os clientes da Akamai frequentemente atacados, representando uma grande variedade de setores como um indicador importante de novos vetores ou tendências de ataque.

### Detecção rápida de ameaças

Nossos novos recursos permitem a rápida implementação de proteções contra ameaças emergentes e CVEs de alto perfil. As atualizações automáticas e a opção de ações “gerenciadas pela Akamai” permitem gerenciar as defesas com agilidade.

## Proteção de CVE

A Equipe de pesquisas sobre ameaças da Akamai continua a monitorar as vulnerabilidades e exposições comuns e garante que a solução WAAP seja atualizada para proteger os aplicativos dos clientes e fornecer a confirmação necessária por meio da ferramenta de pesquisa CVE da Akamai. Essa ferramenta ajuda com informações detalhadas sobre CVEs, incluindo níveis de ameaça e insights sobre as proteções atuais da Akamai. O catálogo de proteção CVE da Akamai permite visibilidade para que você possa priorizar seus esforços de segurança em conformidade com as proteções da Akamai. Além disso, permite pesquisar na base de dados de CVEs para verificar as medidas de proteção ativas da Akamai contra determinada vulnerabilidade, avaliar o nível de ameaça e acessar detalhes do CVE.



# Plataforma de edge globalmente distribuída

## Confiabilidade e resiliência

Soluções WAAP Premium são desenvolvidas em redes amplas e avançadas que não limitam o tráfego bom dos clientes, mesmo nos maiores ataques cibernéticos. A qualidade, a capacidade e a habilidade de execução comprovadas da plataforma global de um provedor de WAAP devem ser igualmente importantes para os recursos da solução. Quando um provedor de WAAP não consegue permitir um tráfego bom durante um ataque ativo, os clientes devem avaliar se investiram em uma solução ou apenas em uma ferramenta.

O compromisso da Akamai é oferecer aos nossos clientes desempenho e proteção líderes no setor. Essa missão só é possível se os serviços forem construídos sobre a mais sólida base: o Akamai Connected Cloud. A Akamai criou a plataforma de nuvem mais distribuída do mundo, composta por mais de 4.200 PoPs de edge, em mais de 130 países.

Os clientes da Akamai incluem todas as 10 principais corretoras, todos os 10 principais bancos, todos os 10 principais serviços de streaming de vídeo e todas as 10 principais empresas de jogos. Nossa base de clientes abrange desde a maioria das principais empresas automotivas, provedores de serviços de saúde, varejo e operadoras de telecomunicações até um número significativo de órgãos governamentais e as forças armadas.

Esses clientes confiam na capacidade da Akamai de fortalecer e proteger contra 40 bilhões de bots por dia, 780 milhões de ataques a aplicativos por dia e 1.889 ataques DDoS por trimestre que ameaçam derrubar suas redes. A Akamai proporciona segurança com sucesso, já que a inteligência contra ameaças obtida por um cliente é usada para beneficiar e proteger todos os clientes. A escala da plataforma global da Akamai oferece a quantidade e a qualidade de dados necessárias para proteger organizações que estão entrando na era da IA.

## Escalabilidade global

Para um WAF, a questão da escalabilidade envolve a capacidade de inspecionar o volume necessário de tráfego da Web, tanto inicialmente quanto à medida que cresce com o tempo, além do número de regras exigidas para avaliar esse tráfego. Soluções WAF tradicionais baseadas em hardware geralmente sofrem com a falta de escalabilidade, pois estão limitadas aos recursos de CPU e memória do dispositivo, podendo ter que competir com outras soluções no mesmo dispositivo.

A implementação de uma solução WAAP integrada na plataforma em nuvem da Akamai elimina problemas de escala ao aproveitar os recursos distribuídos de seus servidores para inspecionar o tráfego da web recebido. Usuários e invasores se conectam a websites protegidos por meio do servidor Akamai mais próximo, que inspeciona o tráfego em busca de ataques e bloqueia todas as solicitações mal-intencionadas detectadas. Isso permite que a solução WAAP da Akamai se ajuste perfeitamente a qualquer aumento na quantidade de tráfego dos aplicativos da Web, sejam picos repentinos de tráfego ou um crescimento a longo prazo, além dos novos locais de usuários em todo o mundo.

## Desempenho

O baixo desempenho pode prejudicar a implementação de uma solução de segurança, especialmente uma solução WAAP implementada em linha na frente de um aplicativo. A redução do desempenho dos websites que são essenciais para os negócios pode levar à diminuição da produtividade, à má experiência do usuário, a um tempo de comercialização mais lento e à redução da receita.

A escalabilidade global da plataforma de nuvem da Akamai permite que a WAAP proteja os aplicativos da Web sem reduzir o desempenho. A WAAP distribuída globalmente inspeciona o tráfego HTTP quando ele chega à plataforma, distribuindo os recursos de CPU e memória necessários para inspecionar esse tráfego em todos os servidores da plataforma. Isso elimina a questão do desempenho como uma fonte de atrito intraorganizacional e uma obstrução à implantação.

## A plataforma de edge fortalece a proteção

Soluções Akamai de segurança de aplicativos da Web independentes da nuvem funcionam perfeitamente em toda a plataforma na defesa contra uma grande variedade de ataques baseados em aplicativos e APIs.

A imagem abaixo ilustra toda a estrutura dos mecanismos e controles de segurança em camadas da Akamai, projetados para manter as ameaças afastadas da origem, ao mesmo tempo em que melhoram o desempenho e o acesso para usuários legítimos.


O Akamai App & API Protector inclui uma grande variedade de mecanismos e controles de segurança incorporados automaticamente (representados em azul) para uma defesa abrangente e pronta para uso, enquanto produtos e serviços adicionais da Akamai são adicionados para uma proteção completa da Camada 7

## Suporte contra ataques gerenciados

Além do gerenciamento constante da WAAP, a Akamai também oferece aos clientes suporte contra ataques gerenciados: monitoramento 24 horas por dia, 7 dias por semana, de websites protegidos e uma resposta gerenciada a qualquer ataque detectado.

Suporte contra ataques gerenciados com a equipe do SOC (Centro de operações de segurança) global da Akamai para responder a incidentes de segurança conforme eles ocorrem, mediante as seguintes ações:

- Responder aos alertas WAAP e às solicitações dos clientes e realizar uma investigação mais detalhada dos problemas
- Determinação da assinatura de ataque adequada e implementação de medidas adicionais de atenuação
- Trabalho com equipes de aplicativos do cliente para medir a eficácia e a precisão das atenuações implementadas, ajustando as atenuações conforme necessário
- Análise da resposta geral com as equipes de aplicativos do cliente após o incidente
- Inclusão de botões de alerta de ataque na interface para iniciar uma solicitação de suporte de emergência

## Centro de comando de operações de segurança (SOCC)

O centro de comando de operações de segurança, ou SOCC (Security Operations Command Center), da Akamai tem ajudado a atenuar muitos dos maiores ataques em todo o mundo há mais de 10 anos, protegendo os clientes de um cenário de ameaças globais em constante evolução.

O monitoramento e a atenuação de ataques mal-intencionados exigem quatro recursos:

- Visibilidade global
- Monitoramento e alertas proativos
- Atenuação ágil de ataques
- Serviço de consultoria constante proporcionado por uma equipe de segurança experiente

O Akamai SOCC oferece esses recursos operando a maior infraestrutura de segurança do mundo. Todo o tráfego de rede é executado em nossa plataforma de segurança unificada, que reúne inteligência em tempo real. Por exemplo, a Akamai reuniu tendências de segurança, como um grande aumento recente nos ataques de injeção de SQL.

Tudo isso ajuda a equipe de segurança da Akamai a atenuar rapidamente as ameaças aos clientes com o máximo de eficácia e o mínimo de impacto.

# Conclusão

Além da proteção contra DDoS na camada de rede e de aplicativos, novas formas de bots automatizados e ataques direcionados por meio de APIs e componentes do lado do cliente significam que as organizações devem proteger todos os aplicativos da Web, endpoints de API, navegadores e infraestrutura com uma abordagem abrangente de segurança de defesa em profundidade. Líderes e profissionais de segurança precisam de uma segurança de aplicativos da Web que identifique e atenue rapidamente as ameaças de vários vetores de ataque, estendendo proteções tradicionais para além do firewall até as tecnologias de segurança adjacentes, a fim de criar a melhor defesa de segurança.

A abordagem da Akamai para a WAAP é oferecer um conjunto de soluções inigualável em sua amplitude e eficácia, com todas as tecnologias de segurança necessárias para uma postura de segurança moderna. Acreditamos que a solução de segurança líder não deve ser apenas para as maiores ou mais populares marcas do mundo. Nosso portfólio para proteções de aplicativos e APIs torna a segurança eficaz de aplicativos da Web disponível para qualquer organização que priorize a segurança por meio de um portfólio em camadas.

Com uma solução de segurança que evolui e se adapta constantemente, agindo com base em inteligência de ataque ampla e profunda, a Akamai faz parceria com empresas globais para modernizar e melhorar constantemente os resultados de segurança. Procuramos capacitar as equipes de segurança da sua organização com a inteligência, a visibilidade, a automação e a orientação para promover iniciativas internas e manter os adversários fora dos seus sistemas corporativos. É por isso que as marcas mais exigentes e que movimentam a vida on-line confiam sua proteção a nós.