Desvendando os cinco mitos sobre Web Application Firewalls (firewall de aplicações da Web)

Para as organizações que conduzem negócios de missão crítica online, o WAF (Web Application Firewall) deve ser a primeira linha de defesa a manter o tráfego mal-intencionado longe, ao mesmo tempo em que permite a passagem do tráfego legítimo. A tecnologia WAF está disponível há muitos anos, e a definição original do WAF é muito simplista por seus usos evoluídos e modernos. Isso faz com que muitos líderes de negócios e profissionais de segurança sustentem percepções e mitos desatualizados.

Esses mitos podem fazer com que as organizações subestimem e subutilizem o poder do WAF que provavelmente já está em sua pilha, abrindo a porta para os invasores e aumentando o risco operacional. A necessidade de segurança digital abrangente da tecnologia WAF continua a crescer. Para melhorar as posturas de segurança e aproveitar as mais recentes proteções da tecnologia WAF, precisamos primeiro abordar os mitos mais comuns.

As tentativas de ataque a aplicações da Web cresceram mais de

300%

na primeira metade de

2022

Fonte: Pesquisa da Akamai sobre ameaças, 2022

Mito 1

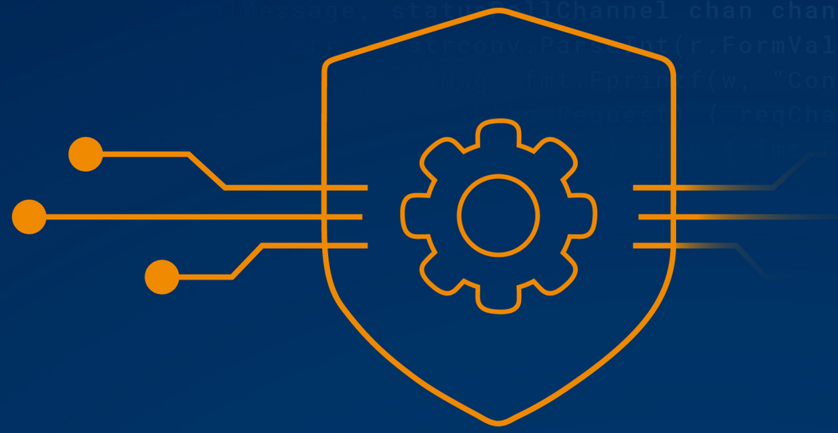
Os WAFs precisam de atualizações manuais constantes para manter a eficiência

Embora seja verdade que as atualizações mais recentes fornecem as proteções mais recentes, há alguns mitos que envolvem esta afirmação que exigem esclarecimento. Atualmente, muitas organizações têm recursos ou experiência em segurança insuficientes para atualizar e ajustar continuamente as regras do WAF. O impacto comercial das atualizações automatizadas e adaptáveis é mais do que apenas economia de tempo e facilidade de uso, trata-se também de redução de riscos. Quando analisamos empresas que optaram por atualizar manualmente, mais de 77% usavam uma versão atrasada em cinco ou mais atualizações do conjunto de regras. Considerando que os clientes da Akamai estavam protegidos contra o Log4j, o maior evento de segurança em 2021, por atualizações automatizadas, fica claro que há risco inerente ao depender de uma abordagem manual. A Akamai envia atualizações WAF de forma contínua e automática, economizando tempo, investimento em recursos e riscos desnecessários para sua organização.

Mito 2

Os WAFs apenas controlam o tráfego

Um WAF legado ficou no meio do tráfego entre os usuários e uma aplicação da Web inspecionando o tráfego HTTP em relação a uma lista definida de regras. Na Akamai, nossa solução inovou de forma rápida e furiosa para além do WAF tradicional para fornecer mais recursos e proteções, incluindo mitigação de DDoS, segurança de API, mitigação de bots, detecção de malware, detecção de dados confidenciais e aceleração de desempenho. E com o lançamento do App & API Protector, sua solução de segurança WAF agora é fornecida com tecnologias ainda mais adoradas pelo cliente, incluindo Site Shield, mPulse Lite, EdgeWorkers, Image and Video Manager, API Acceleration e muito mais. A execução de uma solução WAF pela Akamai é uma tecnologia multifuncional que oferece aos profissionais de segurança visibilidade e controles completos para proteção de segurança em todas as propriedades.



Mito 3

Os WAFs levam ao excesso de alertas do defensor

Pergunte a qualquer defensor da linha de frente, e você ouvirá em primeira mão como as equipes de segurança são sobrecarregadas pelo grande volume de alertas e acionadores necessários para investigar, especialmente aqueles gerados pelas defesas WAF. Resolver esse problema é exatamente o motivo pelo qual a Akamai desenvolveu nosso Adaptive Security Engine, a principal tecnologia que aciona a solução WAF da Akamai. Com o Adaptive Security Engine, sua organização tem proteção moderna possibilitada combinando machine learning, inteligência de segurança em tempo real, automação avançada e percepções de mais de 400 pesquisadores de ameaças da Akamai. Criado para proteger aplicações da Web e propriedades de API por inteiro, o Adaptive Security Engine é único porque aprende padrões de tráfego e ataque específicos para cada cliente, analisa as caraterísticas de cada solicitação em tempo real e usa esse conhecimento para interceptar e adaptar-se a ameaças futuras. Ao contar com o Adaptive Security Engine, os defensores podem dizer adeus ao excesso de alertas, economizando tempo valioso e reduzindo o nível de esforço para manter as aplicações e as APIs protegidas.

As recomendações de ajuste do Adaptive Security Engine demonstraram reduzir falsos positivos em até

5x

Mito 4

Regras WAF mais personalizáveis oferecem mais segurança

Mais regras podem significar mais configuração, mais testes e mais análises. Embora mais regras nem sempre signifique segurança aprimorada, menos regras também não. Se você é o profissional de segurança que acredita que mais é igual a mais, então não se preocupe. Nosso WAF vem com regras personalizadas ilimitadas, e nossas atualizações de regras proativas e adaptáveis são entregues independentemente de quantas você tenha. Com atualizações automáticas e autoajuste automatizado, sua equipe pode verificar de forma eficiente e eficaz a configuração WAF em escala em todo o seu estado digital. Deseja adicionar uma nova regra? O modo de avaliação permite avaliar o impacto de regras novas e modificadas sobre o tráfego ao vivo e ver efeitos em tempo real nos painéis do portal do cliente. Esse estilo de teste de modo de sombra garante que sua nova regra proteja exatamente como esperado na implantação.

Mito 5

Os WAFs só atrapalham um desenvolvedor

Os desenvolvedores impulsionam o valor reconhecido pelo cliente para organizações modernas. Se a segurança atrapalhar, a inovação diminui, os ciclos de lançamento são atrasados e a velocidade de retorno diminui. No entanto, ao mesmo tempo, lançamentos não testados podem criar resultados devastadores de segurança que paralisam as operações comerciais. Na Akamai, somos defensores dos profissionais de segurança e dos desenvolvedores. Acreditamos que as defesas WAF, aquelas que protegem apps e APIs e muito mais, podem permitir que uma cultura do DevSecOps impulsione a velocidade, a agilidade e a colaboração. É por isso que todos os nossos recursos WAF podem ser gerenciados por meio de uma API AppSec ou Terraform aberta que permite que sua equipe automatize a integração de aplicações e APIs, bem como o gerenciamento de configurações de segurança. E quando você precisa de ajuda, o Akamai TechDocs oferece recursos modernos, interativos e intuitivos especificamente projetados para desenvolvedores.

Com superfícies de ataque em rápida expansão e ameaças em constante evolução, combinadas com invasores altamente motivados, os defensores precisam de visibilidade além das proteções WAF tradicionais. Inicie uma avaliação gratuita ou saiba como a Akamai protege seus ativos mais críticos voltados para a Web para reduzir o risco e o atrito operacional de sua organização.

Como a Akamai pode ajudar

Com superfícies de ataque em rápida expansão e ameaças em constante evolução, combinadas com invasores altamente motivados, os defensores precisam de visibilidade além das proteções WAF tradicionais. O Akamai App & API Protector é uma solução única que reúne diversas tecnologias de segurança, incluindo firewall de aplicações da Web, mitigação de bots, segurança de APIs e proteção contra DDoS. Com o App & API Protector, as defesas de segurança são atualizadas contínua e automaticamente, com recomendações de políticas personalizadas implementadas em um só clique. Tecnologia central do App & API Protector, o Adaptive Security Engine oferece proteção moderna combinando machine learning, inteligência de segurança em tempo real, automação avançada e insights de mais de 400 pesquisadores de ameaças.

Inicie uma avaliação gratuita ou saiba como a Akamai protege seus ativos mais críticos voltados para a Web para reduzir o risco e o atrito operacional de sua organização.