PENSE PRIMEIRO NA SEGURANÇA DE APLICATIVOS

ESCOLHENDO O WAF QUE É MELHOR PARA VOCÊ

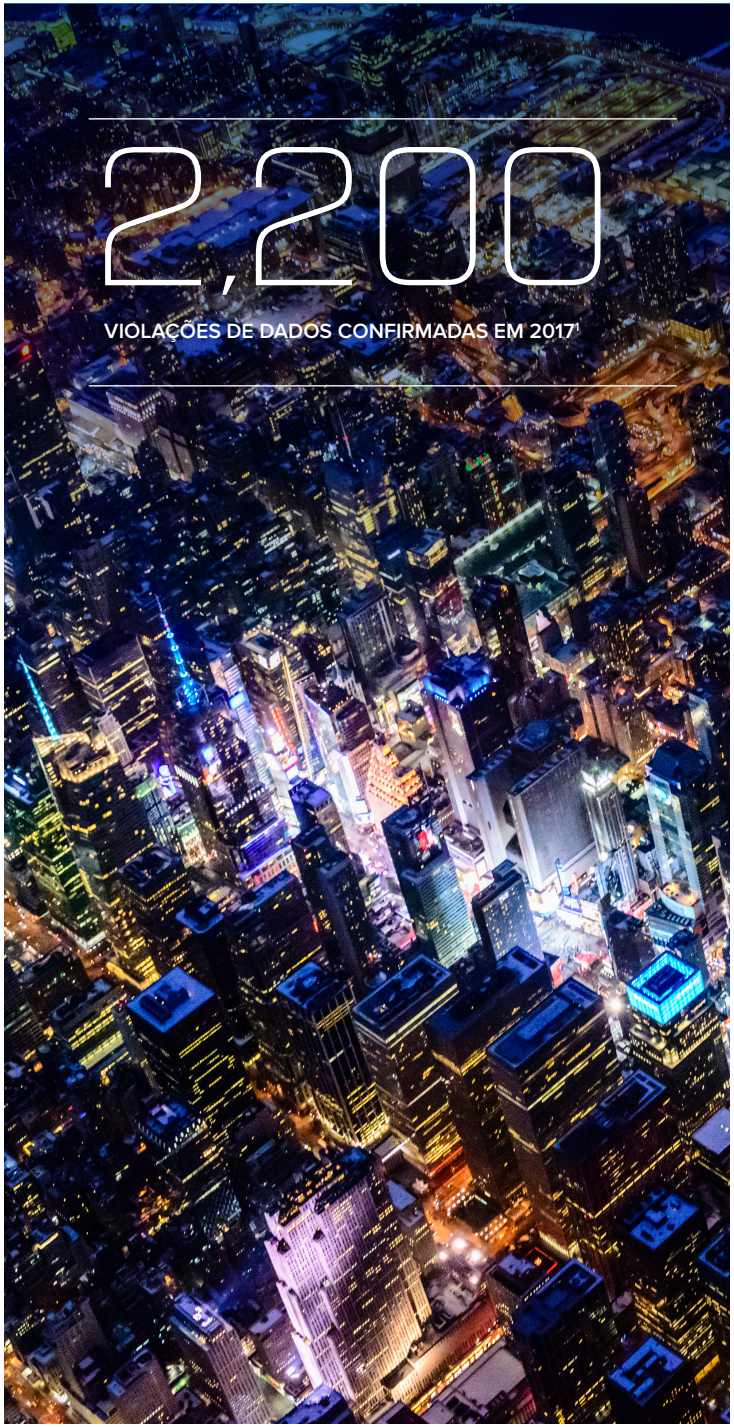
UM GUIA PASSO A PASSO

INTRODUÇÃO

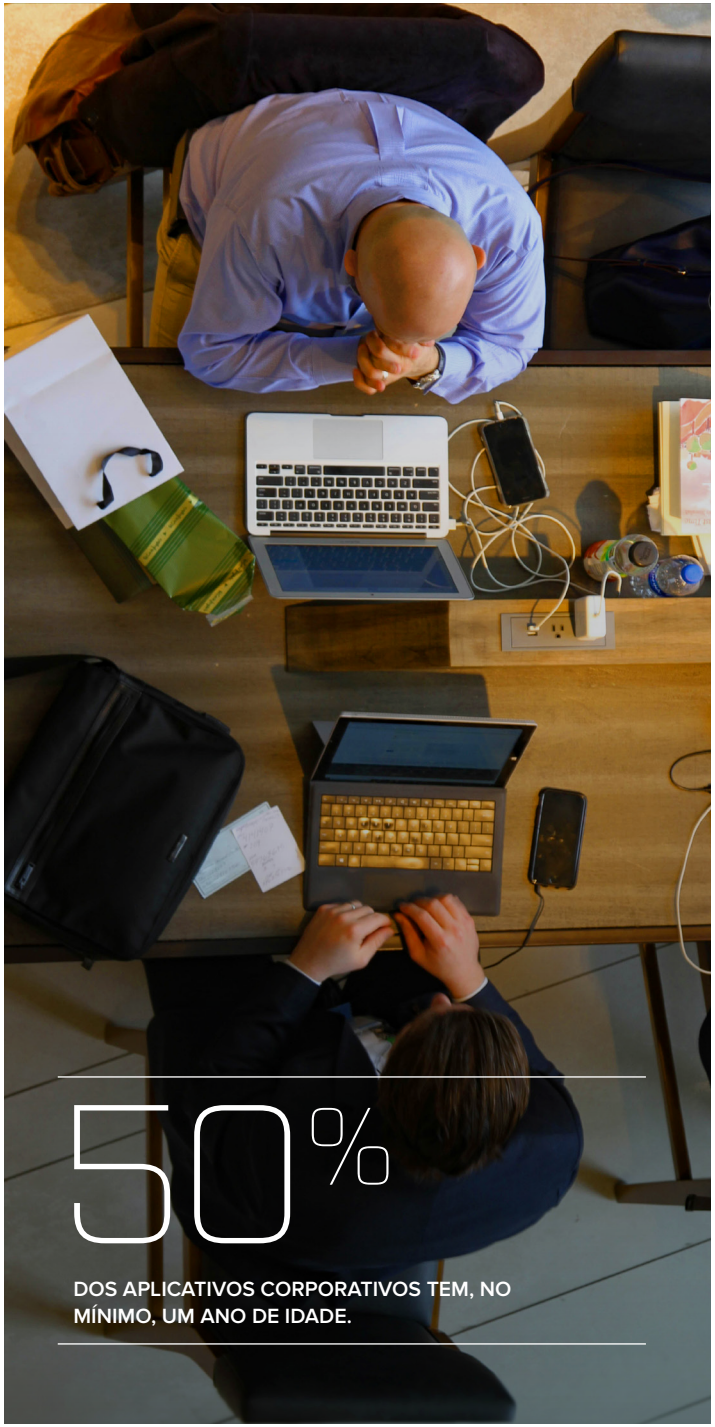
Apesar dos melhores esforços coletivos da indústria de tecnologia para impulsionar as práticas seguras de desenvolvimento de aplicativos, metade de todos os aplicativos permanece vulnerável a ataques.

O Relatório de Investigações de Violações de Dados da Verizon de 2018 revela que, em 2017, havia mais de 2.200 violações de dados confirmadas - e essas são apenas as que conhecemos.[1] Apesar dos melhores esforços do setor de tecnologia para reforçar as práticas de desenvolvimento seguro de aplicativos, metade de todos os aplicativos permanece vulnerável a ataques. Isso não é muito surpreendente - o desenvolvimento seguro de aplicativos Web é notavelmente difícil.[2]

A boa notícia é que existem ferramentas para ajudá-lo a reforçar seus aplicativos contra violações, atenuando vulnerabilidades e interrompendo ataques: especificamente, WAF (Web Application Firewalls). Um WAF inspeciona o tráfego de entrada e saída de aplicativos para identificar e bloquear scanners, invasores e bots, enquanto preserva e acelera aplicativos para uso legítimo. Quer implantada no local, alavancada na nuvem, ou consumida como serviço, a tecnologia WAF pode ajudar a defender sua organização contra ataques a aplicativos Web, que são o principal ponto de entrada de violações de dados bem-sucedidas. [3]



[1] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf
[2] https://www.whitehatsec.com/news/half-of-corporate-web-apps-contain-flaws-that-are-at-least-a-year-old/
[3] https://www.f5.com/labs/articles/threat-intelligence/lessons-learned-from-a-decade-of-data-breaches-29035

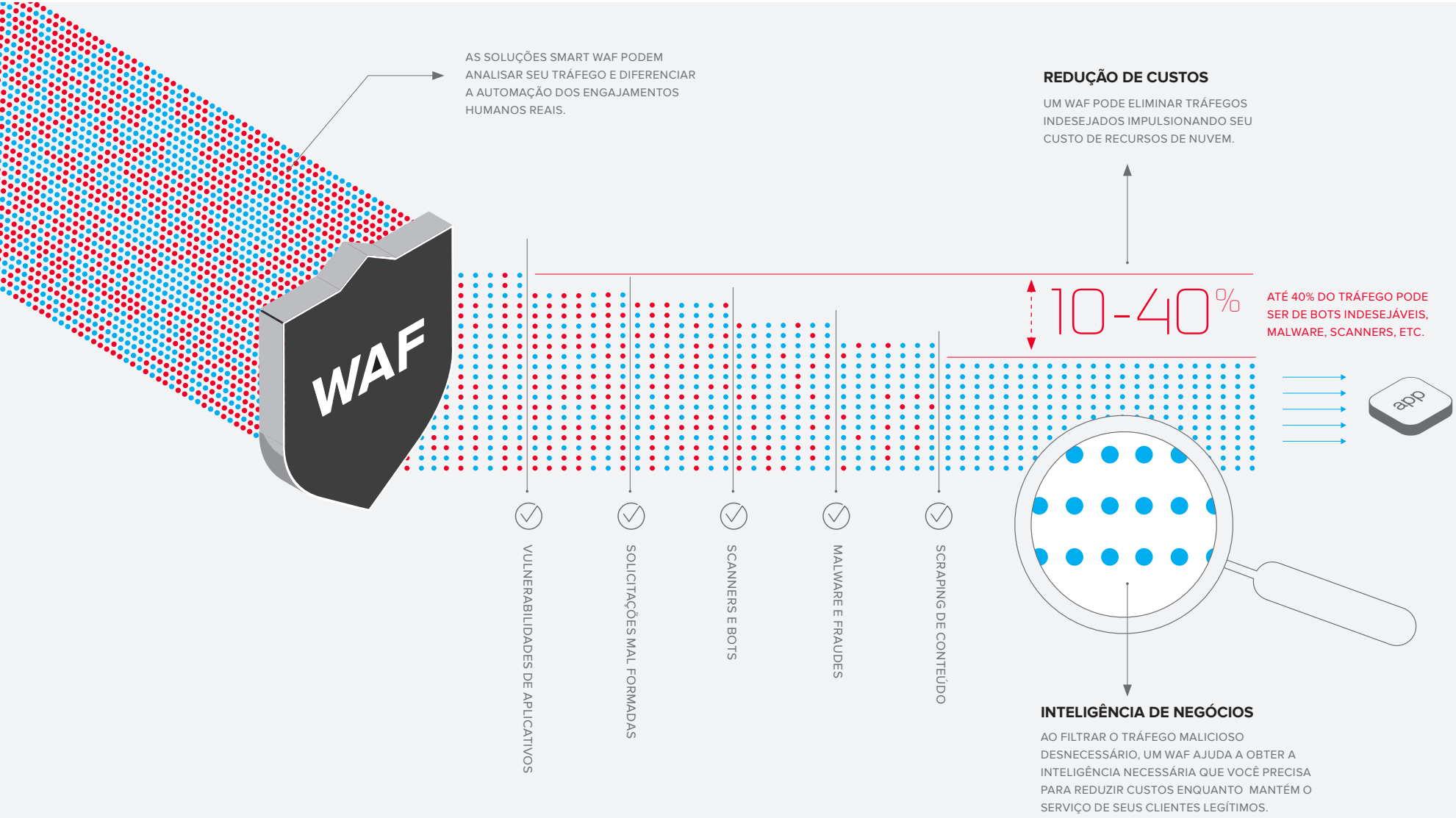


E ENTÃO, VOCÊ PRECISA DE UM WAF? ISSO DEPENDE DE VÁRIOS FATORES.

- Você tem uma propriedade Web voltada para o público?
- Você tem uma propriedade Web de alta sensibilidade?
- Você lida com bots e tráfego automatizado indesejado?
- Você tem obrigações de conformidade?
- Você tem pilhas de softwares de difícil atualização?
- Você aproveita aplicativos Web herdados?
- Você precisa de algum espaço de manobra dos ataques de dia zero?
- Você deseja reduzir o tempo de desenvolvimento para o mercado?

Se você respondeu “sim” a qualquer uma dessas perguntas, você deve considerar a tecnologia WAF ao planejar a proteção de seus aplicativos, de seus dados e de sua empresa contra ataques de aplicativos Web e violações de dados.

Como acontece com qualquer boa ferramenta, há muitas opções - e diferentes soluções funcionam melhor para diferentes situações. Continue lendo para saber a melhor forma de escolher o modelo de implantação do WAF ideal para sua empresa.



UM WAF PODE REDUZIR OS CUSTOS DA NUVEM E IMPULSIONAR A INTELIGÊNCIA EMPRESARIAL

A implantação de um WAF na frente de seu aplicativo baseado em nuvem pode gerar economia e facilitar a obtenção de insights orientados por dados de que sua empresa precisa.

1 FERRAMENTAS INTELIGENTES DE SEGURANÇA PODEM ADICIONAR VALOR REAL AO NEGÓCIO?

Pode ser difícil justificar o gasto com soluções de segurança. Claro, todos nós sabemos que devemos ter medidas defensivas robustas; e esperamos ser protegidos se formos atacados. Mas você nunca sabe se vai ser atacado, muito menos se esse firewall ou IPS será capaz de proteger sua rede com eficiência se você o fizer. A segurança é frequentemente considerada como um mal necessário sem ROI quantificável, mas nem sempre tem que ser este o caso.

No mundo da computação em nuvem e big data, as soluções de boa segurança podem, na verdade, gerar economia ao ajudá-lo a otimizar seus aplicativos Web e propriedades digitais - e elas podem fazer isso enquanto ainda protegem seus negócios contra ataques. As soluções Smart WAF podem filtrar seu tráfego, ajudando você a diferenciar melhor entre bots automatizados e humanos reais. Isso é importante porque, à medida que cada vez mais provedores de serviços baseados em nuvem oferecem um modelo de faturamento de serviços públicos, o tráfego de bots pode aumentar seus custos sem fornecer nenhum valor comercial.

Se você usar um WAF para eliminar grande parte desse tráfego de bots, poderá otimizar suas propriedades Web para a sua base de clientes pretendida, reduzindo o tráfego inútil ou malicioso, resultando em uma economia significativa de custos. Você pode garantir que só estará atendendo seus clientes reais e potenciais, o que significa que suas ferramentas de segurança estão fornecendo valor real, ajudando você a controlar seus custos na nuvem. Além disso, seus dados de interação com o cliente serão aprimorados, resultando em inteligência de negócios mais forte. Quando você tem dados sólidos e acionáveis nos quais confia, você estará em uma posição melhor para comercializar de maneira eficaz com seus clientes reais.

NO MUNDO DA COMPUTAÇÃO EM NUVEM E BIG DATA, BOAS SOLUÇÕES DE SEGURANÇA PODEM REALMENTE GERAR ECONOMIA.

OPÇÕES A CONSIDERAR:

WAF AVANÇADO NO LOCAL (APARELHO VIRTUAL OU DE HARDWARE)

Adicionar valor comercial real além de atuar como uma apólice de seguro em caso de violação. Com defesa proativa de bot combinada com proteção avançada de aplicativos, inteligência contra ameaças e aprendizado de máquina, esse tipo de WAF pode ajudá-lo a reduzir custos na nuvem e refinar sua inteligência de negócios.

BASEADO NA NUVEM + GERENCIADO AUTOMATICAMENTE

Permite cortar custos, refinar sua inteligência de negócios e obter um ótimo valor comercial. Com o mesmo conjunto de recursos que um WAF local, um WAF auto-gerenciado baseado na nuvem oferece proteção de bot proativa, proteção avançada de aplicativos, inteligência contra ameaças e aprendizado de máquina.

2 VOCÊ QUER GERENCIAR SEU NEGÓCIO OU GERENCIAR SUAS SOLUÇÕES DE SEGURANÇA?

De acordo com o Relatório sobre o Estado de Fornecimento de Aplicativos (SOAD) de 2018, da F5, o número de violações aumentou muito no último ano. Com mais violações, há menos confiança na eficácia das soluções de segurança para proteger os dados confidenciais que as organizações processam e mantêm.[4] O problema é que, a menos que você seja um CISO focado exclusivamente em proteger os dados da sua empresa, você provavelmente não quer gastar todo o seu tempo gerenciando as minúcias dos muitos riscos de segurança de aplicativos Web que estão por aí.

É provável que você queira uma solução de segurança que simplesmente funcione, para que você possa se concentrar no desenvolvimento e na implantação de aplicativos essenciais aos negócios, mantendo-os on-line e disponíveis.

Felizmente, várias opções de WAF permitem que você faça exatamente isso. E ainda há mais boas notícias: de acordo com a mesma edição do relatório SOAD, a implantação de um WAF tem um forte efeito no nível de confiança que os entrevistados tinham na proteção de seus aplicativos. Das organizações com uma confiança muito baixa na proteção de aplicativos locais, apenas 6% usavam um WAF. No entanto, daqueles com confiança muito alta, 37% usaram um WAF.[5] Está claro que a implantação de um WAF pode ajudar a proteger seus aplicativos, mas diferentes métodos de implantação são melhores para diferentes organizações.

SE VOCÊ ESTÁ PROCURANDO UMA SOLUÇÃO DE SEGURANÇA QUE APENAS FUNCIONA, EXISTE UMA VARIEDADE DE OPÇÕES QUE PERMITE QUE VOCÊ FAÇA ISSO.

[4] https://interact.f5.com/2018_SOAD.html
[5] https://interact.f5.com/2018_SOAD.html

OPÇÕES A CONSIDERAR:

BASEADO NA NUVEM + TOTALMENTE GERENCIADO COMO UM SERVIÇO

Você pode proteger seus aplicativos Web e os dados contra ameaças em constante evolução oferecendo suporte 24x7. Aumente (ou substitua) seus próprios recursos internos com um serviço totalmente configurado, implantado e mantido por especialistas certificados em um Centro de Operações de Segurança.

BASEADO NA NUVEM + AUTO-PROVISIONADO

Oferece a você o mesmo nível de controle e personalização normalmente oferecido aos aplicativos em um data center privado, ao mesmo tempo em que potencializa a resposta rápida às ameaças direcionadas a aplicativos na nuvem.

WAF AVANÇADO NO LOCAL (APARELHO VIRTUAL OU HARDWARE)

Oferece níveis de controle acessíveis que podem ajudá-lo a atender às suas necessidades de proteção e dar visibilidade do tráfego de aplicativos sem exigir gerenciamento em tempo integral.

3 VOCÊ QUER IR ALÉM DO CUMPRIMENTO REGULATÓRIO BÁSICO?

Muitas organizações se sentem confortáveis com sua postura de segurança existente, mas podem estar considerando a tecnologia WAF como resultado de um mandato de conformidade ou descoberta de auditoria. Vários WAFs de nível de entrada diferentes podem certamente ajudá-lo a dar este “ok” e atender aos requisitos de menor denominador comum; mas as organizações que seguem esse caminho geralmente descobrem que implantar essas medidas básicas tem um custo.

Esses WAFs básicos podem ajudá-lo a passar por uma auditoria, mas eles não são criados com a capacidade de gerenciamento operacional em mente e muitas vezes causam mais dores de cabeça do que “curam”. Além disso, como eles não oferecem o conjunto completo de recursos de um WAF robusto, talvez você não descubra que está fundamentalmente mais protegido, apesar do nível de investimento realizado.

Existe um jeito melhor. Se você precisa de um WAF para atender aos requisitos de conformidade ou marcar um “ok” em algum ponto da auditoria, por que não obter um que ofereça mais do que um mínimo de proteção? Um bom WAF permite que você atenda aos seus requisitos de conformidade, além de oferecer a visibilidade adicional necessária para avaliar adequadamente seu risco real x percepção. E considerando que 44% das organizações relataram pelo menos uma violação em 2017, os resultados podem surpreendê-lo.[6]

UM BOM WAF PERMITE QUE VOCÊ CONHEÇA SEUS REQUISITOS DE CONFORMIDADE ENQUANTO TAMBÉM LHE OFERECE A SEGURANÇA E A VISIBILIDADE ADICIONAL NECESSÁRIA.

[6] https://betanews.com/2018/06/05/organization-data-breaches/

OPÇÕES A CONSIDERAR:

COMMODITY

Pode ajudá-lo a passar por uma auditoria, mas não oferecerá altos níveis de proteção sem um nível significativo de conhecimento de configuração e manutenção contínua, e talvez nem mesmo assim.

WAF AVANÇADO NO LOCAL (APARELHO VIRTUAL OU HARDWARE)

Oferece melhor proteção, lhe proporciona análises refinadas e garante que você não esteja apenas sendo aprovado nas auditorias - você está realmente aumentando a postura de segurança de sua empresa.

BASEADO NA NUVEM + AUTO-GERENCIADO

Um WAF avançado, auto-gerenciado e baseado na nuvem que oferece proteção semelhante à sua contraparte local, oferecendo proteção robusta e análises poderosas que reforçam sua postura geral de segurança.

4 VOCÊ QUER CONTROLAR O TRÁFEGO DE BOT ENQUANTO FOCA NOS SEUS CLIENTES?

Mesmo que você já tenha um processo de desenvolvimento de aplicativos forte e seguro e se sinta razoavelmente confiante na segurança dos aplicativos implantados, é provável que esteja enfrentando outro problema: uma grande porcentagem do tráfego da Web para seu site ou serviço da web provavelmente vem de programas autônomos ou bots. Embora esse tráfego possa parecer legítimo à primeira vista, os cliques de bots não são os mesmos que os cliques de humanos. Tráfego indesejado e não lucrativo pode distorcer sua análise e sua inteligência de mercado inundando seus sistemas com dados artificiais.

Além disso, os invasores adotaram o uso da automação para verificar vulnerabilidades em seus aplicativos, atacar credenciais de conta ou causar ataques de negação de serviço (DoS). Ao implantar um WAF avançado com defesas proativas de bot, você pode interromper ataques automatizados e alavancar uma combinação de técnicas baseadas em desafio e comportamento para identificar e filtrar o tráfego de bots. Essa é uma boa notícia para empresas que lutam para gerenciar a quantidade cada vez maior de atividades de bots em suas propriedades digitais. A tecnologia WAF adaptável pode ajudá-lo a se livrar desta tarefa onerosa, para que você possa se concentrar em atender seus clientes reais.

A TECNOLOGIA WAF ADAPTÁVEL PODE MITIGAR OS EFEITOS DO TRÁFEGO DE BOT INDESEJADO.

OPÇÕES A CONSIDERAR:

WAF AVANÇADO NO LOCAL (APARELHO VIRTUAL OU HARDWARE)

Offers proactive bot protection to defend your apps against layer 7 DoS attacks, web scraping, and brute-force attacks—before they harm your site.

BASEADO NA NUVEM + AUTO-GERENCIAMENTO

Um WAF auto-gerenciado baseado em nuvem também pode fornecer o mesmo nível de proteção proativa contra bots, o que ajuda a defender seus aplicativos contra ataques de força bruta de scraping Web e camada 7 DoS.

BASEADO NA NUVEM + GERENCIAMENTO TOTAL COMO UM SERVIÇO

Protege seus aplicativos Web contra ameaças baseadas em bot, oferecendo suporte 24x7. Ao identificar bots maliciosos que ignoram os métodos de detecção padrão, uma solução baseada em nuvem também pode atenuar as ameaças antes que elas causem danos.

PRÓXIMOS PASSOS:

SELECIONANDO O WAF QUE É CERTO PARA VOCÊ

A principal questão a ser feita ao selecionar um WAF é o nível de envolvimento que você deseja ter na implantação e no gerenciamento.

Um WAF não precisa ser tão difícil de implantar e gerenciar, mas, como qualquer ferramenta, você aproveitará mais dela se usá-la mais. Além disso, determinados vetores de ameaças - especialmente ataques direcionados a uma empresa ou propriedade digital específica - podem ser desafiadores.

Por fim, a visibilidade que você obtém ao implantar um WAF avançado pode ajudar a informar seu processo de tomada de decisões para a segurança de aplicativos e os objetivos gerais de negócios, mas somente se sua organização estiver configurada para aproveitar esses dados.

Vejamos as diferentes maneiras de implantar um WAF, juntamente com os prós e contras associados a cada um dos modos.

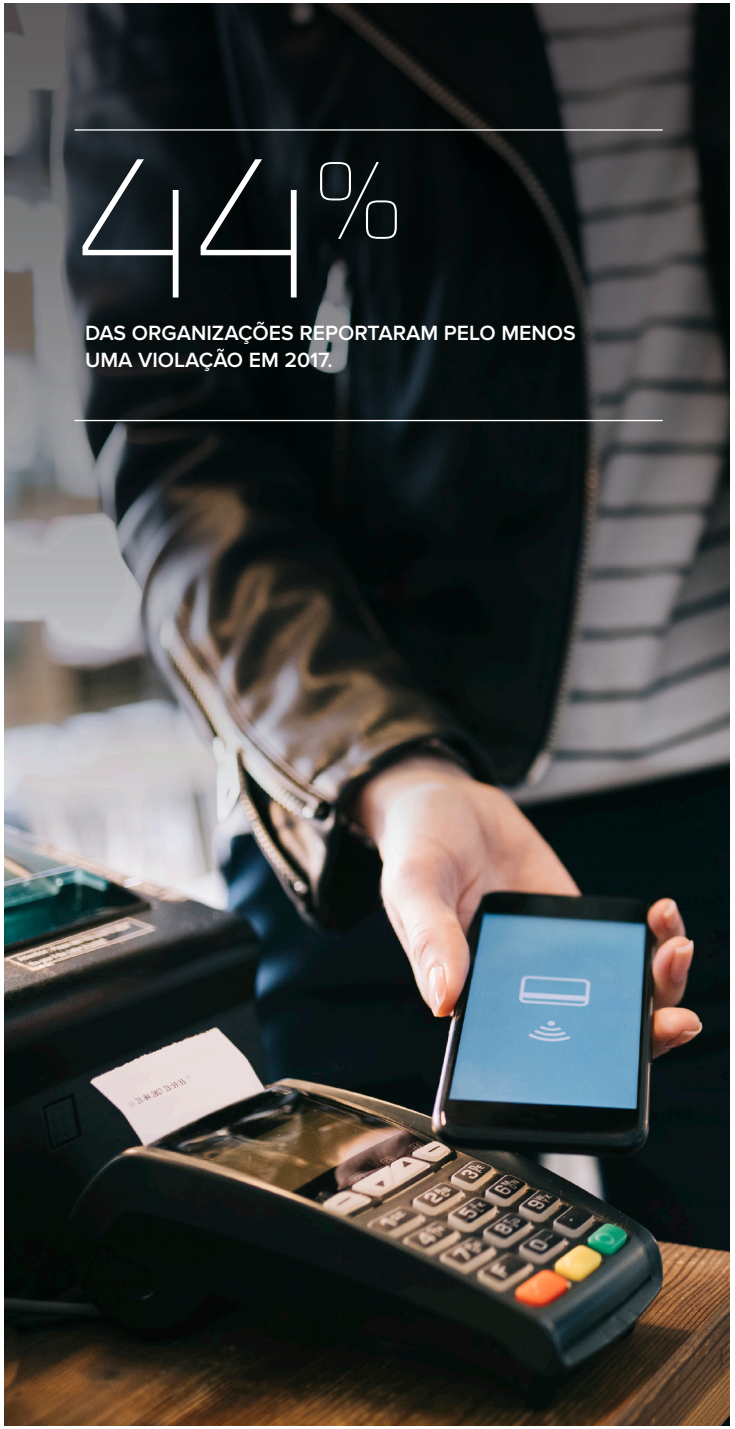
MODOS DE IMPLANTAÇÃO WAF

	PRÓS	CONTRAS	OFERTAS F5
 **BASEADO NA NUVEM + GERENCIAMENTO TOTAL COMO UM SERVIÇOE**	Escolha esta opção se você está procurando a maneira mais rápida e fácil de obter um WAF (e mitigação DDoS) na frente de seus aplicativos.	Embora as ofertas de serviço totalmente gerenciado possam colocá-lo em funcionamento mais rapidamente do que outros modelos, talvez você não tenha tanta flexibilidade arquitetônica. Algumas ofertas podem não lhe dar controle administrativo direto sobre suas políticas de segurança.	WAF Silverline, da F5
 **BASEADO NA NUVEM + AUTO-GERENCIAMENTO**	Obtenha toda a flexibilidade e portabilidade da política de segurança da nuvem, mantendo o controle de suas configurações de política de segurança e gerenciamento de tráfego.	Sendo auto-gerenciado, esse modelo exige algum envolvimento da equipe de segurança e dos proprietários de aplicativos para implantar e criar as políticas de segurança aplicáveis aos seus aplicativos.	WAF Avançado, da F5 Edição BIG-IP na nuvem, da F5
 **BASEADO NA NUVEM + AUTO-PROVISIONADO**	Esta é uma das maneiras mais fáceis de começar com um WAF na nuvem. O aprovisionamento automático permite implementar uma política de segurança que atenda às suas necessidades de maneira fácil e econômica.	Dependendo da arquitetura do seu aplicativo, esse modelo pode não oferecer tanta flexibilidade arquitetônica quanto outros modelos.	WAF para o Centro de Segurança Azure, da F5 WAF Express Silverline, da F5
 **WAF AVANÇADO NO LOCAL (APARELHO VIRTUAL OU HARDWARE)**	Um WAF local (seja virtual ou hardware) pode ajudar a atender a todos os seus modos de implantação mais exigentes, nos quais a flexibilidade de arquitetura, o desempenho e as preocupações com segurança avançada são fundamentais.	Este modelo pode exigir mais investimento inicial em termos de aquisição e implantação do que outros modelos, mas esse investimento pagará dividendos para aqueles que precisam da flexibilidade que ele oferece.	WAF Avançado, da F5
 **COMMODITY**	Este modelo WAF de baixo custo oferece cobertura básica para alguns vetores de ataque conhecidos e pode ajudar a atender aos requisitos de conformidade regulamentar.	WAFs de commodities podem não ter a flexibilidade e a resiliência necessárias para se defender contra os vetores de ameaças em constante evolução que ameaçam negócios de hoje. O mais provável é que este tipo de WAF não o ajude a se defender contra riscos que não são vulnerabilidades de aplicativos, como bots e fraudes.	Regras para AWS WAF, da F5

CONCLUSÃO

Enquanto as escolhas enfrentadas por você possam parecer assustadoras, a verdade é que nunca houve um momento melhor para comprar um aplicativo de firewall Web. A tecnologia WAF agora está mais acessível, econômica e gerenciável que nunca - o que é bom, porque as empresas precisam da proteção que um WAF oferece mais do que nunca.

Para mais informações sobre como escolher o WAF certo para você, visite f5.com/security.



PENSE PRIMEIRO NA SEGURANÇA DO APP

Os aplicativos sempre ligados e conectados podem ajudar a impulsionar e transformar seus negócios - mas também podem atuar como gateways para dados além das proteções de seus firewalls. Com a maioria dos ataques acontecendo no nível do aplicativo, proteger os recursos que impulsionam seus negócios significa proteger os aplicativos que os fazem acontecer.

Sede dos EUA: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Américas: info@f5.com // Ásia-Pacífico: apacinfo@f5.com // Europa / Oriente Médio / África: emeainfo@f5.com // Japão: f5j-info@f5.com

EBOOK-SEC-242055496 08.18