CLOUDFLARE

ARTIGO TÉCNICO

Fazendo mais com menos

Estratégias econômicas de desempenho e segurança de aplicativos de sete empresas.

Conteúdo

Sumário executivo

A maioria das arquiteturas de TI é muito complicada ou desatualizada para aplicar segurança consistente em aplicativos web. As equipes de segurança são forçadas a unir manualmente ferramentas isoladas com visibilidade limitada e controles imprecisos em ambientes de nuvem, híbridos e no local, retardando os negócios.

Toda esta complexidade levou a equipes sobrecarregadas, a vulnerabilidades cada vez maiores, a ataques mais prejudiciais e a um nível insustentável de recursos apenas para acompanhar as ameaças de ontem.

Proteger aplicativos web e APIs contra bots ruins, ataques DDoS, injeção de código e outras vulnerabilidades é uma tarefa crítica para as organizações. No entanto, implementar uma estratégia de segurança de aplicativos robusta pode ser um desafio, especialmente ao lidar com orçamentos restritos e crescimento limitado da equipe.

Este documento compartilha histórias reais de empresas que criaram eficiências e cortaram custos com sucesso em sua estratégia de segurança de aplicativos. Ao aprender com essas histórias de sucesso, as empresas obtêm informações valiosas sobre o uso de práticas de segurança de aplicativos para simplificar as despesas.

Quando as equipes de segurança e TI precisam fazer mais com menos

Quando as organizações enfrentam restrições orçamentárias, nenhuma equipe está totalmente imune. Seja devido à ampla incerteza econômica, queda nas vendas, reestruturação organizacional ou uma série de outros motivos, as equipes de segurança e TI são frequentemente forçadas a melhorar as operações sem o crescimento orçamentário esperado. Ou pior, a fazê-lo ao mesmo tempo em que reduzem os custos.

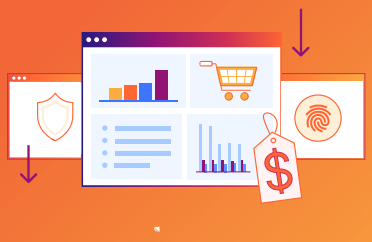
No entanto, a segurança e o desempenho dos aplicativos não são áreas que permitem resultados reduzidos. Do lado da segurança, a proteção de aplicativos fica mais complicada a cada ano. Os ataques ficam maiores e mais complexos do que nunca e, à medida que as organizações escalam, também aumentam suas superfícies de ataque. Por exemplo, houve um aumento de 15% no número de CVEs divulgados entre 2022 e 2023. E apesar de mais de cinco mil vulnerabilidades críticas terem sido divulgadas em 2023, o tempo médio para lançar uma correção para uma vulnerabilidade de gravidade crítica de um aplicativo web permanece consistente por volta de 35 dias, deixando o aplicativo desprotegido durante esse período.

E no lado do desempenho, os consumidores esperam que cada experiência digital seja rápida, confiável e personalizada. Mesmo pequenas desacelerações podem ter um impacto significativo no engajamento e nas conversões do usuário, deixando as empresas em apuros se não conseguirem atender às expectativas de seus clientes.

Ao enfrentar as pressões duplas de restrições orçamentárias e expectativas crescentes, as equipes de segurança e TI precisam encontrar maneiras de entregar mais com menos. Este artigo explora as histórias de empresas que estabeleceram com eficiência uma prática de segurança e desempenho de aplicativos econômica, sem sacrificar os resultados.

Maneiras de reduzir custos em práticas de segurança e desempenho de aplicativos

Quando se trata de proteger aplicativos web e APIs contra ameaças modernas, a melhor defesa não é apenas aquela que oferece serviços de segurança em camadas, mas também aquela que permite que as organizações cortem despesas desnecessárias. Para conseguir isso, as organizações podem usar várias estratégias importantes, incluindo consolidação de fornecedores, gerenciamento simplificado de certificados, proteção dedicada contra ataques que aumentam os custos de tráfego e redução da taxa de saída.



Reduzir os custos com a consolidação de fornecedores de segurança

Simplificar os custos de mão de obra e infraestrutura com o gerenciamento automatizado de certificados

Bloquear ataques que aumentam os custos de tráfego

Eliminar tarifas e custos inesperados, como largura de banda, nuvem e taxas de saída

Reduzir os custos com a consolidação de fornecedores de segurança

Uma pesquisa recente da Gartner afirma que 75% das empresas estão explorando a consolidação de fornecedores em suas práticas de segurança. Ao reduzir o número de fornecedores dos quais dependem, as organizações podem otimizar os processos da cadeia de suprimentos e obter maior eficiência, o que se traduz em redução de custos.

A Chrono24, um marketplace on-line líder de relógios de luxo, reduziu sua dependência de vários fornecedores ao consolidar com a Cloudflare.

Antes da mudança, a Chrono24 usava uma solução de CDN da EdgeCast e mitigação de DDoS e WAF de vários outros fornecedores. A mistura de soluções teve um desempenho insatisfatório, levando a uma latência significativa, baixo desempenho de segurança e desperdício de despesas com fornecedores.

Após a consolidação com as soluções da Cloudflare, incluindo CDN, WAF e mitigação de DDoS, a Chrono24 experimentou uma redução de 67% nos custos de segurança e desempenho do site.

“Nosso custo básico é muito menor agora que consolidamos o desempenho e a segurança em um único fornecedor”, afirma Sven Ferber, Director of Technology. “Eu estimo que estamos gastando cerca de um terço disso.”

A consolidação de fornecedores pode ser uma estratégia altamente eficaz para as empresas otimizarem suas despesas de compras e gerenciamento. Abaixo estão três perguntas rápidas que você pode fazer ao procurar consolidar fornecedores:

1. Seu fornecedor oferece proteção contra ameaças e melhora o desempenho dos aplicativos?
2. Você pode gerenciar seus aplicativos e APIs a partir de um console?
3. Várias equipes em sua organização podem aproveitar o mesmo fornecedor para eficiência de orçamento?

Seguindo as dicas de consolidação acima, as organizações podem reduzir custos, simplificar o gerenciamento da cadeia de suprimentos e fortalecer relacionamentos com fornecedores importantes.

chrono24

Conclusões

75% das empresas estão explorando a consolidação de fornecedores

A **Chrono24** experimentou uma redução de **67%** nos custos com segurança do site e de TI após a consolidação com a Cloudflare

Diminuindo o número de fornecedores e consolidando serviços, as empresas podem **reduzir custos** e simplificar o gerenciamento da cadeia de suprimentos

Simplificar os custos de mão de obra e infraestrutura com o gerenciamento automatizado de certificados

A implantação de configurações de segurança em vários domínios e regiões geográficas pode ser um processo caro e demorado para as equipes de TI. E os custos ocultos podem criar dores de cabeça adicionais para as organizações que elas apoiam, especialmente aquelas que enfrentam restrições orçamentárias.

Frequentemente, esses custos ocultos são disfarçados no gerenciamento de certificados. Os certificados SSL/TLS compõem a identidade digital de uma rede. Em média, a presença na web de uma empresa pode exigir centenas, senão milhares, de certificados. Mas o gerenciamento desses certificados pode ser caro à medida que as despesas de mão de obra e infraestrutura aumentam. Sem mencionar a perda de receita que pode resultar de interrupções inesperadas dos certificados.

A SHOPYY, uma plataforma de comércio eletrônico, usa a Cloudflare para automatizar o gerenciamento de certificados SSL, incluindo criação de chave privada, proteção, validação de domínio, emissão, renovação e reemissão.

Inicialmente, a SHOPYY usou uma ferramenta gratuita de gerenciamento de certificados que fornecia certificados não confiáveis e curtos períodos de validade. Como resultado, a SHOPYY teve que contratar funcionários adicionais para supervisionar o gerenciamento da certificação e o processo de renovação.

Com o Cloudflare SSL for SaaS, a SHOPYY confia o processo de gerenciamento de certificados à Cloudflare, exigindo apenas um funcionário interno para manter todo o processo.

“O uso dos produtos da Cloudflare reduziu os custos em 60% somente em operação e manutenção”, diz o fundador e CTO, Yuanming Chen.

Práticas ineficazes de gerenciamento de certificados também podem afetar a receita devido a certificados expirados. A LendingTree, um marketplace de empréstimos on-line, usa os certificados TLS da Cloudflare para economizar dinheiro e evitar interrupções.

“Temos milhares de ativos diferentes. Nessa escala, era apenas uma questão de tempo até que perdêssemos a renovação de um certificado”, diz o Application Security Lead, John Turner. “Usando os certificados TLS da Cloudflare, que se renovam automaticamente, economizamos cerca de US$ 50 mil por ano, tanto em custos administrativos quanto em perda de receita devido a interrupções por causa de certificados expirados.”

A construção de um sistema eficaz de gerenciamento de certificados também pode ajudar a realocar os recursos adequadamente. Fundada na Alemanha, a mogenius, uma plataforma automatizada que implanta aplicativos baseados em nuvem, automatiza suas práticas de gerenciamento de certificados com a Cloudflare, permitindo que a empresa gaste mais tempo desenvolvendo seu negócio principal.

“Gerenciar tudo o que a Cloudflare faz por nós internamente ocuparia pelo menos 20% do nosso tempo.” Jan Lepsky, cofundador e CPO, relata. **“Com a Cloudflare, podemos nos concentrar em otimizar o desenvolvimento em nuvem e pipelines de implantação para nossos clientes.”**

Remover a carga do gerenciamento de certificados é essencial para empresas que procuram evitar custos ocultos e garantir operações comerciais tranquilas. Práticas de certificação ineficientes, manuais ou mistas levam a altas despesas de mão de obra e infraestrutura, perda de receita devido à interrupção do certificado expirado e desperdício de alocação de recursos.

Ao implementar o gerenciamento de certificados com recursos como certificações SSL for SaaS ou TLS, as empresas podem economizar custos significativos e melhorar seus resultados.

SHOPYY

lendingtree

mogenius®

Conclusões

Usando o Cloudflare SSL for SaaS, a SHOPYY reduziu os custos operacionais e de manutenção em 60%

O Cloudflare TLS ajuda a LendingTree a economizar US$ 50 mil por ano em custos administrativos e perda de receita

A Cloudflare permite que a mogenius automatize suas práticas de gerenciamento de certificados, liberando 20% de seu tempo para se concentrar em seus principais negócios

Bloquear ataques que aumentam os custos de tráfego

À medida que o uso de APIs aumenta, o mesmo acontece com a área de superfície para ataques. Bots maliciosos, ataques DDoS e outras ameaças podem comprometer aplicativos e APIs e os executivos e líderes técnicos estão cientes do impacto significativo que esses ataques podem ter em suas empresas.

De acordo com uma estimativa, descobriu-se que a insegurança de APIs custa às empresas até US$ 75 bilhões anualmente.

Esses ataques resultam em preenchimento de credenciais e ataques DDoS e podem não apenas interromper o serviço para usuários legítimos, mas também forçar as organizações a cobrir os custos de picos de tráfego causados pelo tráfego de ataques.

A LendingTree estava gastando quantias significativas de dinheiro com um fornecedor de segurança anterior que cobrava preços altos durante ataques DDoS. Esse modelo não apenas incorreu em enormes custos excedentes, mas acabou bloqueando o tráfego legítimo.

"Sempre que exibíamos um novo comercial de TV ou uma nova campanha nas mídias sociais, as solicitações disparavam além do limite arbitrário especificado por nosso fornecedor, o que significava que o fornecedor interpretava o aumento como um ataque DDoS e bloqueava o tráfego legítimo", lembra John Turner, Application Security Leader. "**Não apenas perdemos esses clientes em potencial, mas também perdemos o dinheiro que gastamos para levá-los ao nosso site, e nosso fornecedor nos cobrava pela 'proteção contra DDoS'.**"

Para resolver essas ineficiências, a LendingTree recorreu aos recursos de gerenciamento de bots e limitação de taxa da Cloudflare. **Em 48 horas, um ataque a um endpoint de API específico caiu 70% e, em menos de cinco meses, a LendingTree economizou US$ 250 mil ao impedir o abuso de endpoints de API.**

Quando uma holding de jogos on-line, a Flutter Entertainment, percebeu que entre 70 e 90% de seu tráfego era malicioso, eles precisavam de uma solução para filtrar e bloquear bots ruins. Depois de implementar o gerenciamento de bots da Cloudflare, a **Flutter diminuiu o tráfego malicioso em 90%, economizando mais de 2 milhões de libras por ano.**

Usando o gerenciamento de bots e a proteção contra DDoS, as organizações podem evitar ataques e abuso de APIs e reduzir os gastos relacionados a ataques. Ao explorar fornecedores de segurança, as organizações devem procurar fornecedores que:

- Usam aprendizado de máquina para definir limites de taxa com base em dados de tráfego observados.
- Vão além dos limites de taxa baseados em localização de IP e geografia porque os ataques modernos podem contornar os limites de IP facilmente.
- Garantam que os desenvolvedores roteiem todos os aplicativos web e o tráfego de APIs públicas por meio de um WAF e um gateway de API.
- Integram DDoS, WAF e ferramentas de gateway de API para uma defesa contra ameaças em camadas.
- Reduzam a latência garantindo que as proteções estejam em vigor onde a empresa distribui seu tráfego.
- Ofereçam mitigação de DDoS ilimitada para eliminar o pagamento de taxas excedentes.

A implementação da estratégia certa de fornecedor/segurança pode resultar em economia de milhares, senão milhões, de dólares por ano.

Flutter™

Conclusões

Descobriu-se que a insegurança de APIs custa às empresas **até US$ 75 bilhões anualmente**

A implementação das ferramentas de segurança de aplicativos corretas pode resultar em **economia de milhares, senão milhões, de dólares por ano**

Com a proteção contra DDoS, a LendingTree viu um determinado ataque contra API cair 70% em 48 horas e economizou US$ 250 mil em menos de cinco meses ao interromper os ataques

O gerenciamento de bots da Cloudflare ajudou a Flutter a diminuir seu tráfego malicioso em 90% e economizar mais de 2 milhões de libras todos os anos

Eliminar tarifas e custos inesperados, como largura de banda, nuvem e taxas de saída

Muitos serviços de segurança dependem da nuvem, e muitos provedores de nuvem cobram das empresas pelo armazenamento e computação. Além disso, eles geralmente exigem que as empresas paguem taxas de saída de dados, que são despesas associadas à transferência de dados do armazenamento.

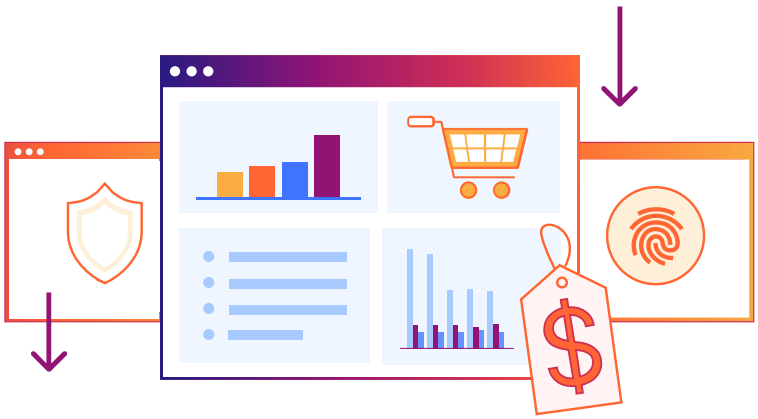
As taxas de saída são calculadas de acordo com vários fatores, como nível do cliente, tipo de assinatura e volume de dados transferidos. Por esses motivos, essas taxas tendem a ser difíceis de prever, o que pode prejudicar as organizações quando elas começam a acrescentar. Na verdade, o IDC estima que as cobranças de taxas de saída representam pelo menos 6% dos custos de armazenamento em nuvem.

Com isso em mente, a PagesJaunes, um diretório digital europeu e serviço de pesquisa local, decidiu implementar a CDN da Cloudflare para ajudar a reduzir as taxas de largura de banda e melhorar o gerenciamento de cache e DNS.

"Percebemos rapidamente que o tráfego absorvido pela CDN da Cloudflare significava que nossa infraestrutura estava menos estressada e mais resiliente", insiste Loïc Troquet, Head of Architecture, Performance and Security. "**70% da largura de banda não precisava mais ser distribuída pela infraestrutura da Solocal.**"

E economia de largura de banda resulta em economia de custos. Depois de adotar os serviços de mitigação de DDoS, CDN, DNS e WAF da Cloudflare, a ferramenta de aprendizado e estudo on-line Quizlet **economizou mais de 10 TB de largura de banda total todos os dias e reduziu a conta de saída de rede do Google Cloud Services em mais de 50%.**

A implementação de estratégias e práticas de segurança de aplicativos pode eliminar taxas de saída inesperadas.



PagesJaunes

Quizlet

Conclusões

A implementação de estratégias de segurança de aplicativos, como a escolha do fornecedor de CDN certo, pode eliminar taxas de saída inesperadas

Com a CDN da Cloudflare, a PagesJaunes reduziu sua largura de banda em 70%

A Quizlet usou a Cloudflare **para economizar mais de 10 TB de largura de banda total todos os dias** e reduzir a conta de saída de rede do Google Cloud Services em mais de 50%, resultando em milhares de dólares economizados todos os meses

Simplificar a segurança de aplicativos e corte custos com a Cloudflare

Com a Cloudflare, as organizações podem criar estratégias de segurança de aplicativos para aumentar a eficiência e simplificar as despesas. O portfólio de segurança de aplicativos integrado da Cloudflare reúne a melhor proteção contra DDoS não medida da categoria, um firewall de aplicativos web que interrompe os ataques mais avançados, segurança de APIs proativa, gerenciamento de bots respaldado por inteligência contra ameaças e detecção avançada de ataques do lado do cliente.

Tem interesse?

Contate a Cloudflare hoje

CLOUDFLARE

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

BDES-5972.2024MAY31