Monetização das soluções Arbor Networks para serviços gerenciados de proteção contra DDoS

DE ACORDO COM UM RECENTE ESTUDO FEITO PELA INFONETICS RESEARCH:

A receita de serviços gerenciados de segurança aumentará 40% ao longo dos próximos 5 anos para US$ 22,2 bilhões no ano de 2019.

Serviços de segurança gerenciados de nuvem e CPE anuais e mundiais e previsões e dimensão do mercado regional: 2015

OUTRO ESTUDO REALIZADO PELA FROST & SULLIVAN (ANÁLISE DO MERCADO DE MITIGAÇÃO DE ATAQUES DE NEGAÇÃO DE SERVIÇO (DDOS) DISTRIBUÍDOS GLOBALMENTE, JULHO DE 2014) INDICA QUE:

"O risco de DDoS e, consequentemente, a demanda para mitigação de DDoS é cada vez maior devido a(o):

- Crescimento máximo e médio de ataques DDoS
- Maior frequência de ataques DDoS, incluindo técnicas de ataque DDoS mais sofisticadas
- Ferramentas de ataque e serviços de contratação permitem uma maior faixa de agentes de ameaça
- Um novo elemento de roubo de dados e intrusão de rede associado aos ataques DDoS."

ARBOR NETWORKS
The Security Division of NETSCOUT

Necessidade crescente de serviços de proteção contra DDoS

Os fatos são claros: ataques DDoS continuam crescendo em tamanho, frequência e complexidade. Em virtude disso, houve um aumento na demanda por serviços de proteção contra DDoS. De acordo com o *11º Relatório de Segurança de Infraestrutura Mundial* anual da Arbor Networks, 78% dos provedores de serviço tiveram aumento na demanda para serviços de proteção contra DDoS.

Por quê?

Para maior proteção DDoS, as práticas recomendadas do setor sugerem fazer uma combinação integrada de proteção contra DDoS no local e na nuvem. Em outras palavras, as empresas não conseguem fazer isso por conta própria e precisam da ajuda de seus provedores de serviço para pôr fim aos ataques DDoS modernos.

De acordo com um recente estudo feito pela Infonetics Research (*Serviços de segurança gerenciados de nuvem e CPE anuais e mundiais e previsões e dimensão do mercado regional: 2015*), a receita de serviços gerenciados de segurança aumentará 40% ao longo dos próximos 5 anos para US$ 22,2 bilhões no ano de 2019. O relatório também declara que:

> *"Apesar de melhorar o quadro econômico global de maneira lenta, o mercado de serviços de segurança gerenciados (particularmente o segmento de nuvem) é forte e está crescendo devido a (entre outras coisas) um aumento no volume, na variedade e na complexidade de ameaças de todos os tipos, que vão desde ameaças em níveis de infraestrutura, como ataque DDoS (que estão se tornando cada vez mais elaborados), a ataques extremamente direcionados usando mais de cinco vetores e adaptando técnicas com base na proteção detectada."*

É evidente que há uma demanda crescente para serviços de proteção contra DDoS. Esse artigo dará instruções sobre como fornecer serviços de proteção contra DDoS gerenciados que só se tornam possíveis com os produtos e serviços da Arbor Networks.

Práticas recomendadas para por um fim em ataque DDoS = oportunidade para provedores de serviços

Os ataques DDoS modernos são uma combinação dinâmica de 1) ataques volumétricos, 2) ataques de exaustão de estado e 3) ataques na camada de aplicativo. As práticas recomendadas do setor sugerem que, a fim de obter uma proteção ampla contra os ataques DDoS modernos, as organizações implementem proteções em camada com suporte para inteligência contra ameaças.

Em outras palavras: A melhor solução para pôr fim a grandes ataques volumétricos é sinalizar para a rede do provedor de serviços antes que eles sobrecarreguem os sistemas no local ou a conectividade de internet local. O melhor local para interromper os ataques furtivos na camada de aplicativo é na localidade do cliente, perto de onde os principais aplicativos e serviços residem. No entanto, também é muito importante que a solução tenha comunicação inteligente entre essas duas camadas com o suporte da moderna inteligência contra ameaças a fim de dar um basta aos ataques DDoS dinâmicos e de multivetor.

TODOS OS SERVIÇOS GERENCIADOS DE PROTEÇÃO CONTRA DDOS SÃO DIFERENTES.

Isso é devido ao fato de que vários fatores influenciam o projeto, a embalagem e os preços de um serviço gerenciado de proteção contra DDoS.

CLOUD SIGNALING COALITION

Atualmente, mais de 60 provedores de serviços fornecem serviços de proteção contra DDoS com base na tecnologia da Arbor.

Eles incluem:

- Axtel
- Aixit
- Allstream
- Bezeq International
- Bharti Airtel
- CAT Telecom
- Circular/Depulsio
- Colt
- Embratel
- FASTWEB
- Hellenic Telecommunications
- Organization (OTE S.A.)
- Jaguar Network
- NextGen Networks
- Gen-I
- Neo Telecoms
- NexusGuard
- Optus
- OrangePolska
- Starhub
- Swisscom
- Tata Communications
- Telefonica
- TelstraClear
- True Internet Co. Ltd
- Vocus

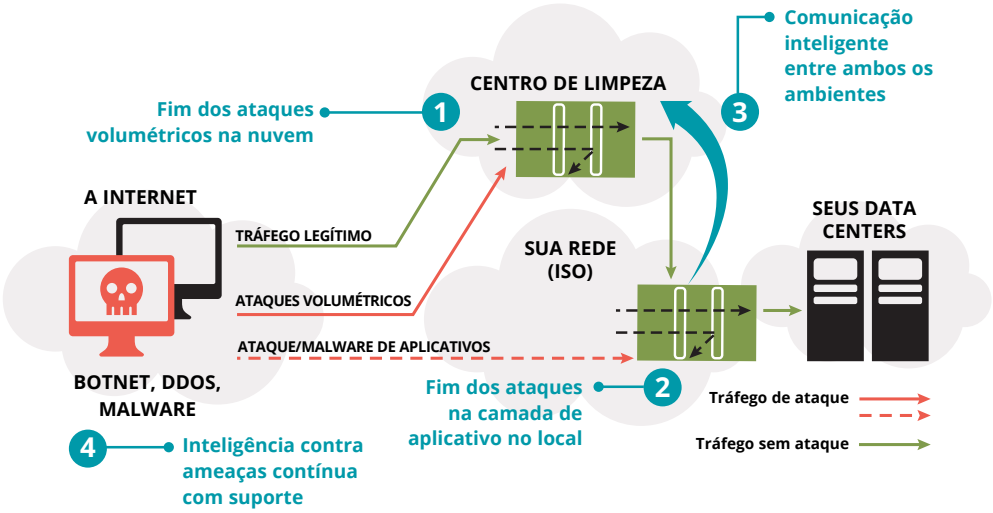

Figura 1: *Práticas recomendadas para maior proteção contra DDoS*

Monetização dos serviços de proteção contra DDoS

Como observado anteriormente, os provedores de serviço estão bem posicionados para fornecer soluções de proteção contra ataque DDoS em camadas. Nos últimos 15 anos, a Arbor Networks tem sido a líder absoluta nos serviços, produtos e pesquisas de ataque DDoS. Atualmente, mais de 60 provedores de serviços fornecem serviços de proteção contra DDoS com base na tecnologia da Arbor. Listados à esquerda estão alguns desses provedores que também são membros da Cloud Signaling Coalition da Arbor.

A Arbor Networks tem o maior portfólio de proteção do mercado de serviços e produtos de proteção contra DDoS. Abaixo segue uma breve descrição dos produtos e serviços da Arbor.

Arbor SP e Threat Management System (TMS)

- O Arbor SP fornece visibilidade de rede dominante e detecção de ataque DDoS.
- O Arbor TMS fornece mitigação cirúrgica, fora da banda e sem estado de ataques DDoS que chegam até 160 Gbps.

Arbor Availability Protection System (APS)

- Detecção e mitigação de ataques DDoS sempre ativas e em linha que vão desde sub 100 Mbps a 40 Gbps.
- O Cloud Signaling fornece integração inteligente com o Arbor Cloud.
- Disponível como um dispositivo 2U ou plataforma virtual com serviço gerenciado opcional.

Arbor Cloud DDoS Protection Service

- Combinação de proteção contra DDoS no local e na nuvem totalmente integrada e gerenciada.
- Mais de 1 Tbps de capacidade de limpeza global e ISP agnóstico localizada nos Estados Unidos, Europa e Ásia.

O diagrama na próxima página representa uma possível implementação de soluções de proteção contra DDoS da Arbor. Todas elas podem ser personalizadas e monetizadas a fim de fornecer um serviço de proteção contra DDoS para seus clientes.

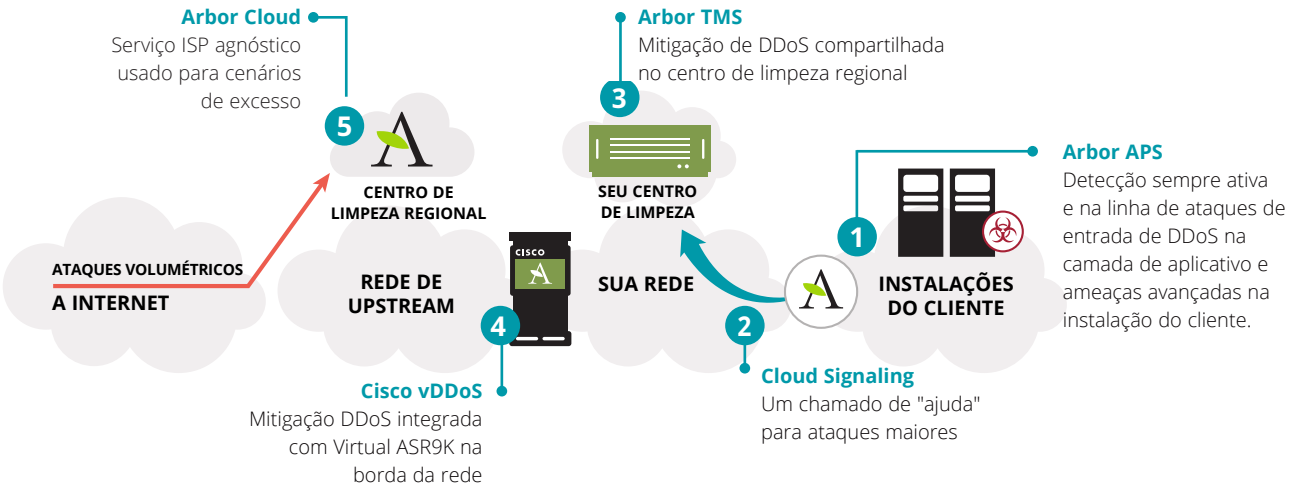

Figura 2: *Maior capacidade de mitigação na nuvem*

Componentes comuns de um serviço de proteção contra DDoS

Todos os serviços gerenciados de proteção contra DDoS são diferentes. Isso é devido ao fato de que vários fatores influenciam o projeto, a embalagem e os preços de um serviço gerenciado de proteção contra DDoS. Com isso em mente, há alguns componentes que são comuns na maior parte dos serviços de proteção contra DDoS. São eles:

- Na nuvem ou no local
- Sob demanda ou assinatura
- Detecção de ataque ou mitigação
- Acesso aos portais do cliente e relatórios
- SLA, termos legais e condições de serviço

A tabela abaixo mostra como esses componentes comuns são geralmente usados para fornecer diferentes serviços de proteção contra ataque DDoS. O número de sinais de dólar ($) denota a diferença relativa em preços dos serviços.

RECURSOS	Emergência *Sob demanda*	Assinatura *Bronze*	Assinatura *Silver*	Assinatura *Gold*
Na nuvem: Mitigação **sob demanda de ataques DDoS**	✓			
Na nuvem: Detecção **proativa** de DDoS, geração de relatórios		✓	✓	✓
Na nuvem: Mitigação **proativa** de ataques DDoS, geração de relatórios e portal do cliente			✓	✓
Baseado em CPE: Detecção e mitigação **proativa** de ataque DDoS				✓
Na nuvem + CPE: Mitigação **proativa** de excesso de fluxo e Cloud Signaling de grandes ataques DDoS				✓
PREÇO	**$$$**	**$**	**$$**	**$$$**

SERVIÇOS DE ASSINATURA

É importante observar que esses diferentes serviços são resultado da monetização de diferentes recursos das soluções de proteção contra DDoS da Arbor Networks e/ou Cisco. (Consulte a tabela à esquerda para ver os produtos de proteção contra DDoS da Arbor Networks e Cisco).

Por exemplo:

- **Assinatura Bronze**: Serviço de detecção proativa de ataque DDoS na nuvem; pode ser fornecido usando o software Arbor Networks SP.
- **Assinatura Silver**: Serviço de detecção e mitigação proativa de ataque DDoS na nuvem; pode ser fornecido usando a combinação do software Arbor Networks SP, além da linha de produtos de proteção Cisco vDDoS Protection e Arbor Networks TMS (para mitigação).
- **Assinatura Gold**: Combinação de serviços de mitigação e detecção de ataque DDoS na nuvem; (fornecido usando os componentes da assinatura Silver) além de uma solução de proteção contra ataque DDoS no local que se conecta à solução em nuvem durante ataques grandes; fornecido usando o Arbor Networks APS, Cloud Signaling, além dos produtos mencionados na assinatura Silver.

PRÓXIMAS ETAPAS

Whitepaper da Frost & Sullivan

Chamado de "O crescente papel do provedor de serviços na mitigação de DDoS", ele explica o papel fundamental que as MSSPs podem desempenhar na proteção corporativa contra DDoS.

Vídeo da solução TMS e Arbor SP

Um vídeo que descreve os principais recursos e benefícios da solução de proteção contra DDoS da Arbor.

Consultoria gratuita sobre DDoS

Para obter uma consultoria gratuita sobre DDoS a fim de aprender ainda mais sobre como proteger a sua rede e gerar receita de serviços de proteção contra DDoS, entre em contato com o seu representante local da Arbor ou Cisco.

ARBOR NETWORKS

The Security Division of NETSCOUT

Sede corporativa
76 Blanchard Road
Burlington, MA 01803 USA
Chamada gratuita
dos EUA: +1 866 212 7267
Tel.: +1 781 362 4300

www.arbornetworks.com

Vendas na América Latina
Brasil
T: +55.11.4380.8035
brasil@arbor.net

Mexico, Caribe & América Central
T: +52.55.4624.4842
mxcca@arbor.net

América Latina do Norte
T: +57.1.508.7099
nola@arbor.net

América Latina do Sul
T: +54.11.5218.4007
sola@arbor.net

DS/SPMONETIZATION/PT/1016-LETTER

Preços dos serviços de proteção contra DDoS

Assim como não existe uma abordagem "tamanho único" ao projeto e embalagem dos serviços de proteção contra DDoS, o mesmo se aplica ao preço desses serviços. Definir preços é uma decisão exclusiva de cada empresa. Para determinar o preço adequado para serviços, é necessário considerar vários fatores, como:

- Seus clientes-alvo: Para quem você planeja vender esses serviços e qual é a vontade deles de consumir esses serviços? Você possui serviços gerenciados de segurança (por exemplo, firewalls ou IPS gerenciados) dos quais pode tirar ideias? Ou você baseará o serviço DDoS como uma elevação percentual ou taxa fixa com base nos circuitos de internet existentes que você vende atualmente (por exemplo, serviços de proteção contra DDoS não podem custar o triplo do preço dos circuitos de internet)?
- Sua concorrência: À medida que mais clientes começam a exigir serviços de proteção contra DDoS, mais e mais concorrentes entrarão no mercado. Você conhece a sua concorrência? Você sabe qual é o preço e o pacote de serviços que eles oferecem?
- Sua empresa: Cada empresa possui um conjunto diferente de requisitos de receita e lucratividade. Isso terá um impacto no preço do seu serviço.

Outras práticas recomendadas para fornecer serviços de proteção contra DDoS

Há muito mais a se considerar no desenvolvimento de um serviço de proteção contra DDoS. Abaixo seguem algumas outras considerações e práticas recomendadas.

- **SLAs e contratos**: Contratos de Acordo de nível de serviço (SLA) e Descrição de serviços, componentes muitas vezes não valorizados dos serviços de proteção contra DDoS. Esses documentos fundamentais descrevem exatamente os serviços que a sua organização fornecerá. Eles são exclusivamente criados de acordo com a concepção dos seus serviços, nível de experiência, tamanho da equipe de mitigação de DDoS etc.
- **Equipe e processo**: Os melhores serviços de proteção contra DDoS no mundo possuem equipes dedicadas e processos bem documentados. Além do mais, esses processos são constantemente testados (por exemplo, em brincadeiras internas de disputa) e redefinidos para garantir que as equipes e o serviço sejam otimizados.
- **Tamanho e excesso de assinaturas**: Você precisa considerar o quanto de capacidade será necessário para lançar o serviço inicialmente e qual será a taxa de excesso de assinaturas determinada para o planejamento de crescimento à medida que o seu negócio se desenvolve. Uma taxa de 10 para 1 geralmente é usada e pode mudar ao longo do tempo dependendo da sua dimensão, do risco que os clientes têm de serem atacados, do tamanho dos ataques e do tamanho da sua largura de banda para fazer upstream de provedores de serviços, hospedagem, propriedades da web etc.
- **Dê passos curtos:** Se você é novo no ramo de serviços de proteção contra DDoS, é recomendável que você comece com uma base de clientes ou geografia limitada antes de entrar de cabeça em serviços completos e abrangentes. Isso permite que você aprenda, refine o seu processo e também justifique a expansão do serviço.

Conclusão

Já fizemos isso antes... entre em contato conosco para saber mais.

Nos últimos 15 anos, a Arbor Networks têm excedido as demandas das redes de provedores de serviços mais desafiadoras do mundo. Essas operadoras confiam na Arbor Networks para proteger sua disponibilidade e oferecer o portfólio de proteção contra DDoS mais confiável, testado e seguro a fim de proteger seus clientes e ganhar dinheiro com isso. Não é à toa que a Arbor é sempre chamada para proteger as Olimpíadas. Nós ajudamos todos os tipos de provedores de serviços de todos os tamanhos e de todas as partes do mundo. Estamos prontos para ajudar você a fornecer os serviços de proteção contra DDoS que são certos para os seus clientes e organização. Entre em contato conosco quando estiver pronto para dar o próximo passo e suprir a demanda dos seus clientes em relação à proteção contra DDoS.