Proteção contra DDoS em um mundo de nuvem híbrida

Índice

O DDoS continua evoluindo

O DDoS (Negação de serviço distribuído), um dos tipos mais antigos de ciberameaça, continua evoluindo e agora se tornou uma ferramenta altamente sofisticada nas mãos de cibercriminosos e hacktivistas com motivações ideológicas. De fato, os ataques DDoS representam riscos de segurança não apenas para grandes e pequenas empresas, mas também para a infraestrutura pública essencial em áreas como saúde, energia e serviços de utilidade pública e educação.

Para complicar ainda mais essa dinâmica, há o aumento da adoção de recursos de computação em nuvem por instituições públicas e privadas. Quando essas organizações combinam a nuvem com seus recursos pré-existentes no local, o ambiente híbrido resultante se torna significativamente mais complexo. Aplicativos, APIs (interfaces de programação de aplicativos), dados, microsserviços e cargas de trabalho agora devem transitar por um ambiente fragmentado. As diferentes arquiteturas desses ambientes criam novas vulnerabilidades e uma superfície de ataque fragmentada que pode ser explorada por cibercriminosos para lançar ataques DDoS cada vez mais sofisticados e debilitantes.

As organizações estão se esforçando para garantir que sua infraestrutura digital esteja protegida. Elas precisam de uma plataforma de proteção contra DDoS integrada e híbrida, que possa proteger sua infraestrutura local (nuvem privada) contra ataques DDoS curtos e incisivos, mas que também aproveite a escala e a capacidade de depuração da nuvem para ataques DDoS volumétricos de grande porte.

As tendências sugerem que os ataques DDoS continuarão a se tornar mais poderosos e mais frequentes. Em fevereiro de 2023, a Akamai mitigou o maior ataque DDoS já lançado contra um cliente Akamai Prolexic baseado na região Ásia-Pacífico (APAC), com um pico de tráfego de ataque de 900,1 gigabits por segundo e 158,2 milhões de pacotes por segundo (Mpps). Isso foi apenas alguns meses após o maior ataque DDoS contra um cliente da Akamai Prolexic na Europa, no qual o tráfego aumentou abruptamente para 704,8 Mpps em uma tentativa agressiva de interromper as operações comerciais da organização. Isso se soma ao maior ataque DDoS que a Akamai mitigou até o momento: um ataque distribuído globalmente de 1,44 terabit por segundo (Tbps) e 385 Mpps que durou quase duas horas. Na verdade, com base em nossa visão sobre os padrões de tráfego e ataque, a Akamai determinou que, ao longo de 2023, ataques DDoS se tornaram mais frequentes, mais longos, altamente sofisticados (com múltiplos vetores) e se concentraram em alvos horizontais (atacando vários destinos IP no mesmo evento de ataque).

A ameaça crescente

Atualmente, a maioria dos ataques DDoS são multivetoriais, muitas vezes empregando mais de 10 vetores de ataque para sobrecarregar sistemas e plataformas rudimentares de proteção contra DDoS. De fato, de acordo com a inteligência interna de ameaças da Akamai, o número de ataques DDoS horizontais ou multidestinos dobrou de 2022 para 2023. Enquanto isso, o tamanho geral, a escala e a duração dos ataques DDoS volumétricos em 2023 foram os mais altos já registrados.

O que complica ainda mais o planejamento da segurança para as organizações é a evolução de várias táticas diferentes que os invasores estão usando em conjunto com os ataques volumétricos tradicionais.

Invasores que utilizam DDoS atacarão qualquer possível ponto de falha, como:

- Websites
- Aplicativos da Web e outros serviços empresariais
- Concentradores de VPN para acesso remoto a recursos corporativos
- Controladores SD-WAN
- APIs (interfaces de programação de aplicativos)
- DNS (Sistema de Nomes de Domínio) e servidores de origem
- Infraestrutura de rede e data center

Infraestrutura de DNS

Os ataques DDoS à infraestrutura de DNS de uma organização têm se tornado cada vez mais comuns, principalmente os ataques NXDOMAIN (também conhecidos como ataques de subdomínio pseudoaleatórios, ataques de tortura de água de DNS ou ataques de esgotamento de recursos de DNS). Mais de 60% dos ataques DDoS mitigados pela Akamai em 2023 tinham um componente DNS, com ataques NXDOMAIN constituindo aproximadamente metade desses ataques DDoS de DNS. Esses ataques representam um risco significativo para os resultados e para a reputação de uma empresa, pois se o DNS de uma empresa cair, sua presença on-line desaparecerá.

Ataques na camada de aplicativo

Os ataques DDoS na camada de aplicativo (Camada 7) se tornaram mais sofisticados, pois os invasores estão desenvolvendo suas táticas para explorar fluxos de trabalho e lógica aparentemente benignos. Uma vulnerabilidade de HTTP/2 descoberta em 2023 levou ao maior ataque DDoS de Camada 7 já registrado.

DDoS como serviço

Grupos cibercriminosos organizados, como o Anonymous Sudan e o Killnet, estão oferecendo DDoS como um serviço. Nesse cenário, os grupos oferecem seus serviços, normalmente uma botnet, por uma comissão e realizam ataques em nome de um cliente. Esses serviços de DDoS por encomenda podem ser extremamente lucrativos para grupos motivados.

Ransomware + DDoS = RDDoS

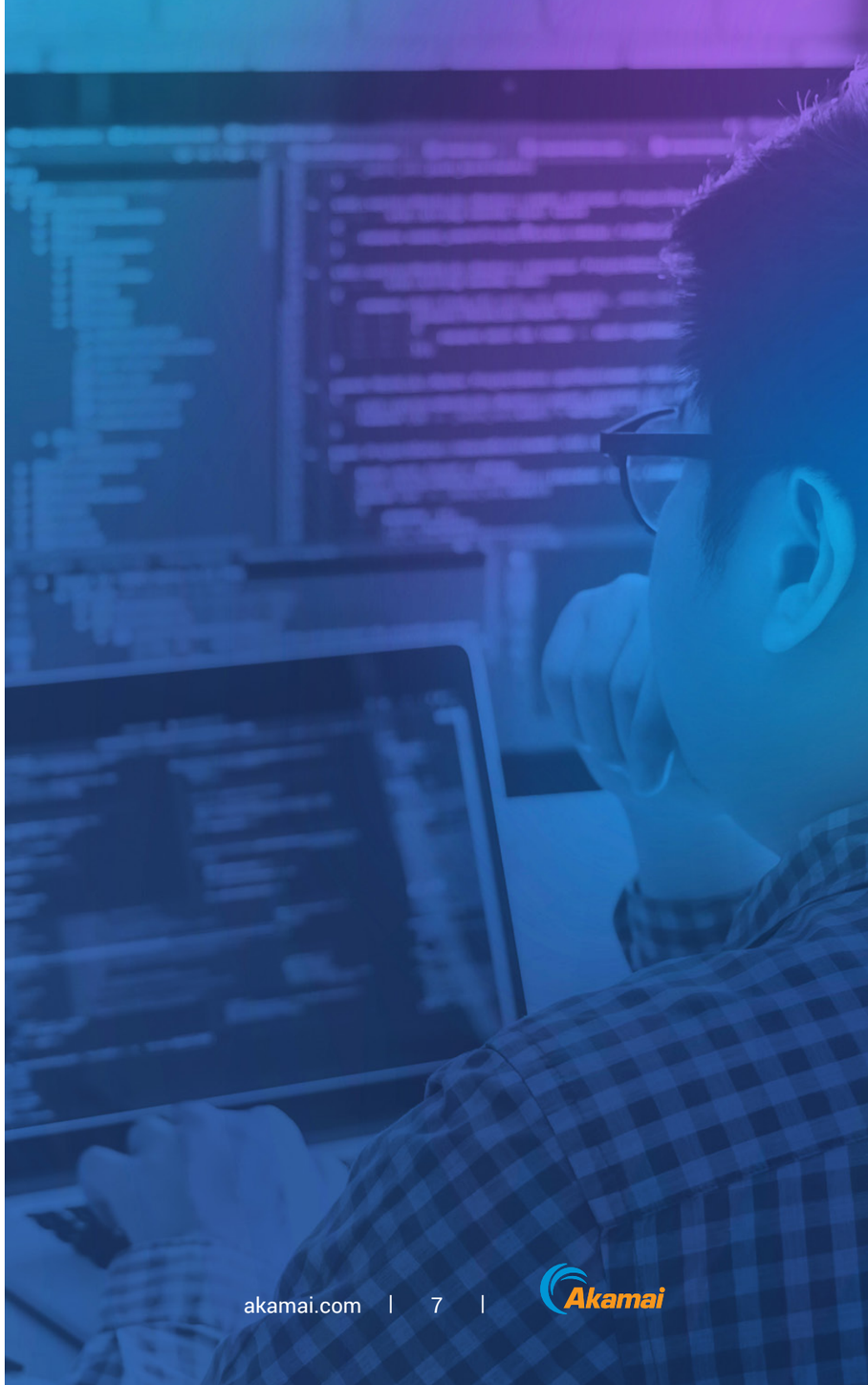
A disponibilidade de táticas como DDoS como serviço também torna mais fácil para os invasores usarem ataques DDoS como cortina de fumaça para distrair as equipes de segurança. Enquanto isso, eles lançam um ataque simultâneo de ransomware ou um ataque de extorsão tripla. Eles são chamados de ataques DDoS com resgate (RDDoS).

As consequências de um ataque DDoS

Com os ataques DDoS nas camadas de rede (Camada 3) e de transmissão (Camada 4), os ataques volumétricos e baseados em protocolo tentam preencher os canais da Internet, sobrecarregar os servidores e esgotar as entradas da tabela de estado para tornar as redes e os serviços indisponíveis. Com os ataques da Camada 7, os agentes de ameaças pretendem atrapalhar o desempenho da Web e a experiência do usuário por meio de vetores, como ataques de baixa intensidade e inundações de HTTP, para gerar tempo de inatividade que afeta os resultados financeiros. Os ataques DDoS ao DNS podem ser um pouco mais complexos: dependendo do tipo de ataque, ele pode afetar diferentes camadas da rede de uma organização. Por exemplo, os ataques DDoS de reflexo e amplificação de DNS podem produzir tráfego nas camadas 3 e 4 da rede de uma empresa, enquanto os tipos de DDoS de inundação de DNS ou NXDOMAIN geralmente atacam a camada de aplicativos de uma rede.

As repercussões do tempo de inatividade afetam mais do que apenas o custo de serviços interrompidos e dos aplicativos indisponíveis. De acordo com o Ponemon Institute, o custo médio de um ataque DDoS em uma organização é de US$ 1,7 milhão por ano, impulsionado pelo aumento do suporte técnico, consumo de recursos de resposta a incidentes, escalonamentos internos, custos legais, interrupção operacional e perda de produtividade dos funcionários. Além disso, para empresas voltadas para o consumidor, como instituições de serviços financeiros, empresas de jogos e mídia e organizações de comércio eletrônico, ficar off-line pode não apenas causar danos financeiros, mas, mais importante, pode causar danos irreparáveis à reputação.

Então, fica evidente que os riscos são altos e estão aumentando com a maior migração para infraestruturas em nuvem híbrida.

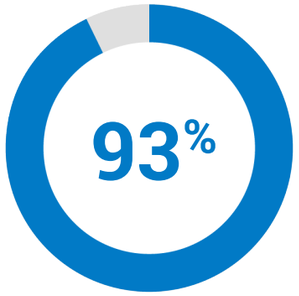


A nuvem híbrida e a multinuvem continuam complicando a segurança

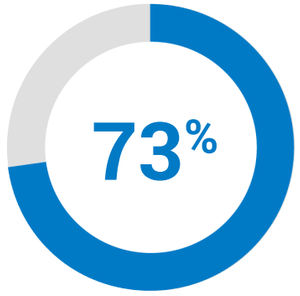
Como as organizações mantêm algumas cargas de trabalho em data centers locais ou nuvens privadas e transferem outros aplicativos para ambientes hospedados em nuvem pública, essa abordagem híbrida da infraestrutura torna extremamente complexo garantir uma segurança robusta. Da mesma forma, as empresas geralmente têm uma infraestrutura de DNS híbrida na qual algumas de suas zonas de DNS autoritativas são gerenciadas na nuvem, com as zonas restantes gerenciadas por servidores de nomes locais e balanceadores de carga de servidor global (GSLBs). Há motivos pelos quais as organizações podem continuar mantendo alguma infraestrutura de DNS no local. Por exemplo, elas podem já ter investido um capital significativo na configuração de uma infraestrutura local para atender aos requisitos de conformidade. A complexidade de migrar todo o DNS para a nuvem pode não ser financeiramente viável.

Os agentes de ameaças estão bem cientes das vulnerabilidades que surgem de um ambiente tão fragmentado. Eles estão ansiosos para explorar as fraquezas da arquitetura e postura de segurança de uma organização, que são criadas por políticas e requisitos de segurança inconsistentes. Eles procuram tirar proveito das dificuldades na solução de problemas em infraestruturas hospedadas em nuvem desiguais e fragmentadas.

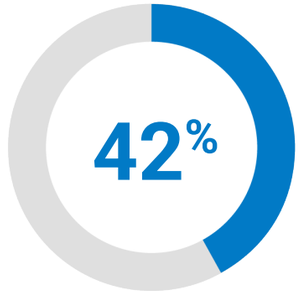
Infelizmente, a responsabilidade pela segurança nos ambientes de nuvem pública pode ser inconsistente e variar de provedor para provedor. Muitas organizações fazem falsas suposições que podem deixar esses ambientes expostos. Por exemplo, 73% dos entrevistados do setor empresarial em uma pesquisa da IBM acreditam que os CSPs (provedores de serviços em nuvem pública) são a principal parte responsável pela proteção do SaaS (software como serviço), enquanto 42% acreditam que os CSPs são os principais responsáveis pela proteção da IaaS (infraestrutura como serviço) em nuvem. Essa falta de conhecimento sobre a responsabilidade do controle de segurança pode gerar comprometimentos, um risco que nenhuma organização deve estar disposta a aceitar.



Empregam uma estratégia multinuvem



Acreditam que os CSPs de nuvem pública são responsáveis por proteger o SaaS



Acreditam que os CSPs são responsáveis por proteger a IaaS em nuvem

As organizações estão se voltando para provedores de proteção contra DDoS que oferecem uma plataforma de proteção contra DDoS integrada, altamente escalável e abrangente, que pode proteger seus aplicativos, APIs, DNS e a infraestrutura subjacente que alimenta tudo isso.

As estratégias de mitigação de DDoS não são todas iguais

Como as empresas continuam investindo em infraestrutura de nuvem, garantir controles consistentes que abranjam ambientes híbridos será um desafio para as equipes de segurança. E, já que fica mais difícil proteger os aplicativos implantados em várias infraestruturas em nuvem de back-end, muitas organizações buscam um ponto único de controle para organizar as defesas.

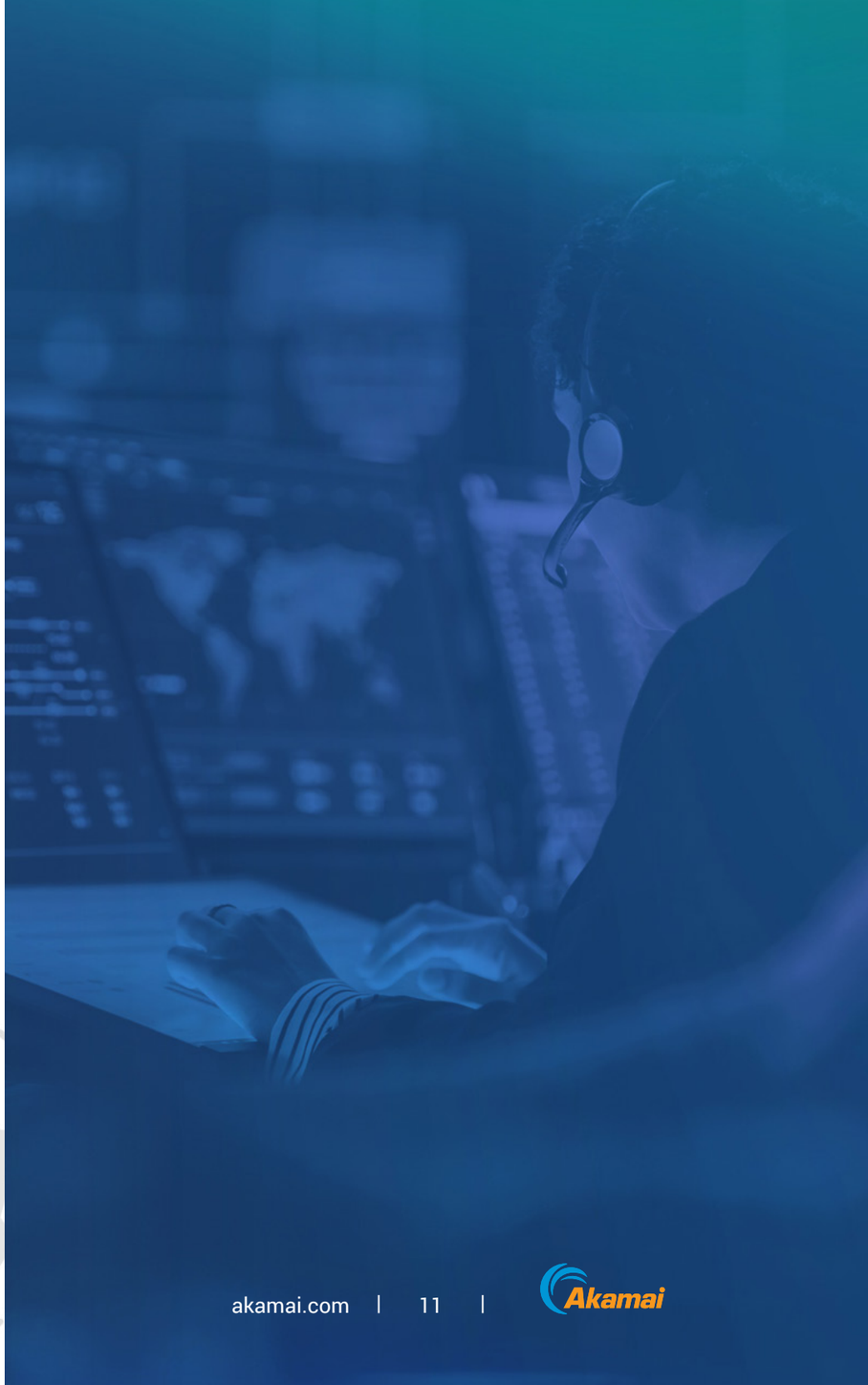
À medida que a pilha de tecnologia de segurança se torna mais complexa, muitos desejam obter uma visão consolidada do ambiente, não apenas para otimizar a visibilidade, mas também para gerar relatórios simplificados que possam ser alimentados por APIs em sistemas de correlação de dados de eventos.

Para resolver este problema, as organizações estão se voltando para provedores de segurança contra DDoS que oferecem uma plataforma de proteção contra DDoS integrada, altamente escalável e abrangente, que pode proteger seus aplicativos, APIs, DNS e a infraestrutura subjacente que alimenta tudo isso. Elas querem defesas escaláveis e responsivas, independentemente de onde os serviços corporativos possam residir, no local, na nuvem ou em um ambiente híbrido. Isso é uma resposta direta ao aumento da complexidade operacional necessária para integrar, implementar e gerenciar as defesas contra DDoS no ambiente exclusivo de um CSP. E com muitos ativos voltados para a internet localizados em várias nuvens privadas e públicas, a complexidade surge rapidamente.

Para piorar, muitas soluções internas de mitigação de DDoS dos CSPs ficam para trás em áreas principais: visibilidade, SLAs (contratos de nível de serviço) e geração de relatórios, que são essenciais para capacitar os atuais defensores empresariais.

Para as equipes de segurança, tudo se resume em visibilidade e em obtenção de insights úteis para otimizar a preparação e a resposta a incidentes. Algumas soluções de DDoS dos CSPs oferecem pouca ou nenhuma transparência em termos de geração de relatórios, visibilidade e análise pós-ataque. Não é de se admirar que muitas equipes se refiram aos CSPs como a caixa preta da análise e geração de relatórios. Embora alguns CSPs permitam que a equipe de segurança de uma organização defina controles e mantenha a soberania de ambientes específicos do cliente, eles normalmente rejeitam qualquer responsabilidade pelo tráfego de DDoS e acabam cobrando dos clientes pelo volume astronômico de tráfego mal-intencionado que vem com um ataque DDoS, seja ou não um ataque na camada de aplicativos, um ataque na camada de rede ou um ataque DDoS de DNS.

Além disso, alguns CSPs e fornecedores de segurança não oferecem um SLA claro de tempo para mitigação (TTM) e, em vez disso, oferecem créditos de serviço para a organização afetada. É importante entender se a cláusula de TTM inclui o tempo para identificar um ataque. Se uma plataforma levar vários minutos ou até horas para identificar um ataque DDoS antes que seus protocolos de mitigação entrem em ação, a organização vítima poderá ficar off-line por um período prolongado. Quando os segundos contam, as organizações precisam ter certeza de que seu provedor se comprometerá a manter o tempo de atividade e a disponibilidade sem comprometer o desempenho.



Além disso, é igualmente (ou até ainda mais) importante que as equipes de segurança ou as organizações compradoras identifiquem se os fornecedores de segurança contra DDoS e os CSPs oferecem **capacidade de defesa contra DDoS** dedicada ou se a capacidade de defesa é compartilhada com a rede CDN (Rede de Entrega de Conteúdo). A defesa dedicada contra DDoS é como uma equipe da SWAT que se concentra exclusivamente no combate a ataques DDoS e não compartilha recursos ou infraestrutura com outros aspectos de uma empresa, como a entrega de conteúdo, garantindo assim um impacto mínimo mesmo durante um ataque DDoS recorde. As organizações que estão avaliando a proteção DDoS precisam entender que os próprios fornecedores, às vezes, enfrentarão ataques DDoS e devem considerar seriamente se o fornecedor oferece um SLA de tempo de atividade/disponibilidade.

Por fim, muitos CSPs e fornecedores de segurança não oferecem acesso sob demanda ao suporte do SOC (Centro de operações de segurança) global 24 horas por dia, 7 dias por semana, além da assistência antes, durante e depois dos ataques. E, quando oferecem, isso terá um custo premium que, muitas vezes, é mais caro do que uma solução de mitigação de DDoS híbrida especializada de um dos melhores provedores do setor. Com uma solução de proteção contra DDoS híbrida totalmente gerenciada, os provedores de serviços atuam como a extensão da equipe de resposta a incidentes de uma organização e oferecem os conhecimentos especializados para responder rapidamente aos eventos de DDoS.

No atual cenário de ameaças, está claro que as empresas modernas estão recorrendo a parceiros de atenuação de DDoS que oferecem suporte a uma experiência de segurança simplificada, em ambientes híbridos, e reduzem a complexidade da superfície de ataque. Seu parceiro de proteção contra DDoS deve ser um facilitador, e não um obstáculo, para sua estratégia híbrida ou multinuvem e estar alinhado com suas metas de negócios.

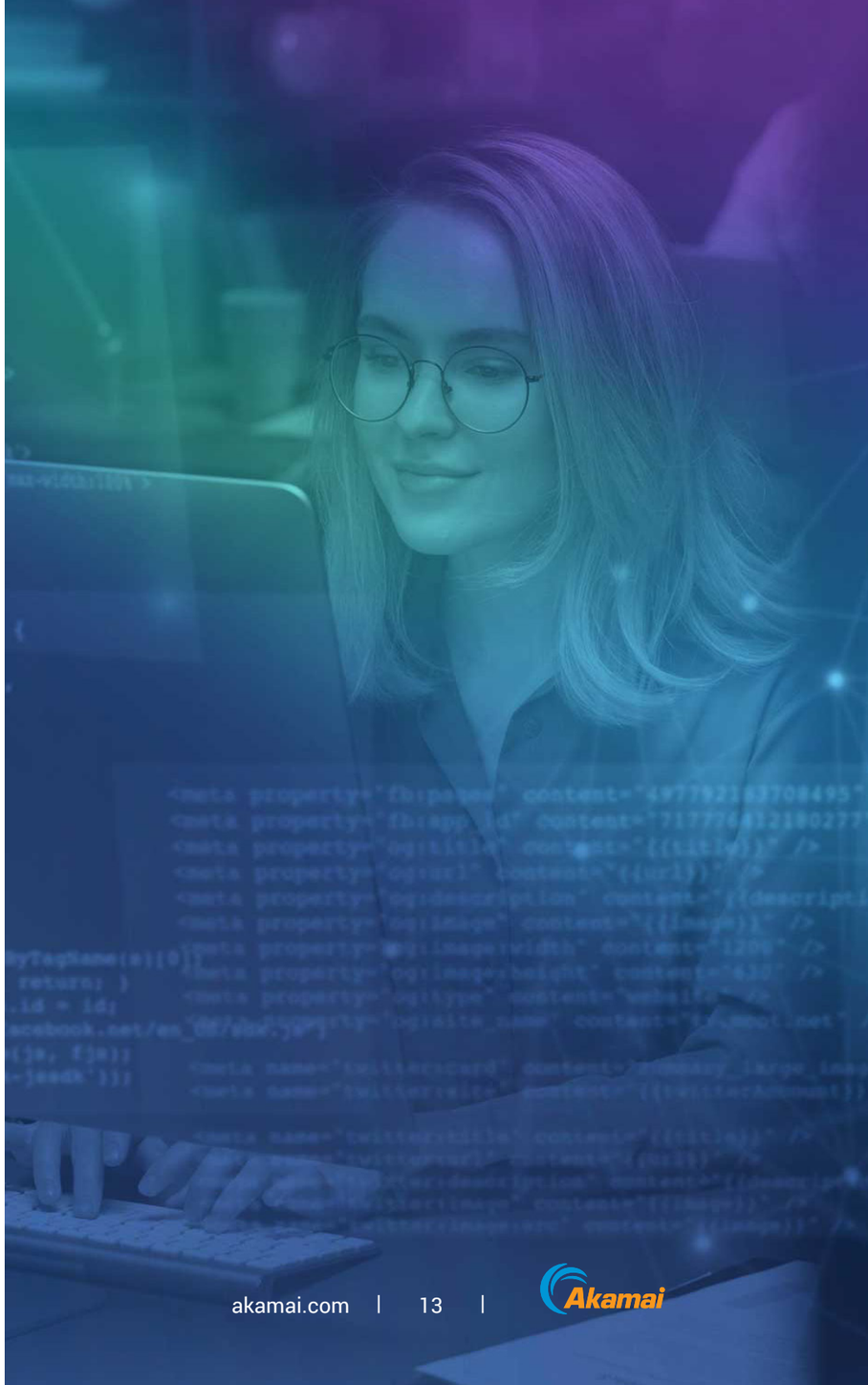
Mitigação de DDoS criada para fins específicos com a Akamai

Assim como as organizações precisam de uma estratégia de infraestrutura digital completa que inclua ambientes híbridos e multinuvem, elas também precisam considerar uma proteção completa contra DDoS. Ao adotar uma abordagem abrangente, a Akamai atua como a primeira linha de defesa, fornecendo proteção com estratégias de mitigação dedicadas híbridas, de DNS distribuído e de edge, criadas para evitar danos colaterais e pontos isolados de falha. Ao contrário de outras arquiteturas de CSP, criadas como uma solução completa, as soluções DDoS específicas da Akamai oferecem maior resiliência, capacidade dedicada de defesa contra DDoS e uma maior qualidade de atenuação, que é ajustada aos requisitos específicos de aplicativos da Web ou serviços baseados na Internet.
A defesa contra DDoS da Akamai está disponível para os clientes onde eles precisam: no local, na nuvem e em ambientes híbridos; e como eles precisam: sempre ativa ou sob demanda. Essa proteção abrangente se apresenta através de três produtos principais.

Capacidade dedicada de defesa contra DDoS

DNS distribuído

Mitigação híbrida



Akamai Prolexic é uma proteção contra DDoS de excelência mundial adaptada à postura de segurança proativa e positiva de uma organização

Uma arquitetura moderna e escalável

O Akamai Prolexic usa uma arquitetura totalmente definida por software, que pode se adaptar às tendências de rede em constante mudança relacionadas à edge computing, 5G/6G e virtualização de rede. Com a transição para ambientes de software virtualizados, o Prolexic removeu todas as dependências de hardware especializado. Essa implantação padronizada permite que a Akamai atenda às crescentes necessidades dos clientes com mais rapidez, facilite implantações modulares para ampliação da capacidade, forneça melhor cobertura regional com links de baixa latência e melhore a redundância na plataforma. Além disso, a arquitetura ajuda a acelerar os recursos avançados de aprendizagem comportamental do Prolexic para aprender com assinaturas de ataque, adaptar-se a vetores de ameaças emergentes e criar de forma proativa posturas resilientes a DDoS para os clientes. A nuvem do Prolexic é alimentada por vários **centros de depuração em 32 áreas metropolitanas globais e um total de mais de 20 Tbps de capacidade de defesa dedicada**. Para colocar a capacidade de defesa do Prolexic em perspectiva, até mesmo os maiores ataques DDoS conhecidos das Camadas 3 e 4 não compõem 10% da capacidade disponível para os clientes do Prolexic.

Proteção abrangente, flexível e confiável contra DDoS

O Akamai Prolexic está disponível como Prolexic Cloud, Prolexic On-Prem e Prolexic Hybrid.

O **Prolexic Cloud** é pioneiro no setor em proteção contra DDoS baseado em nuvem e oferece aos clientes mitigação em zero segundo e SLAs de 100% de disponibilidade da plataforma. Os controles de mitigação dimensionam a capacidade de forma dinâmica para interromper ataques entre os fluxos de tráfego IPv4 e IPv6. Os recursos de computação podem ser alocados dinamicamente para qualquer controle de mitigação que precise ser dimensionado.

O **Prolexic On-Prem** oferece proteção contra DDoS sempre ativa, física ou lógica, em linha e de datapath, que se integra nativamente aos roteadores de edge para interromper automaticamente mais de 98% dos ataques na edge da rede do cliente, sem a necessidade de backhaul de tráfego. Isso é ideal para a grande maioria dos ataques pequenos e rápidos e para empresas que exigem proteção contra DDoS de latência ultrabaixa.

O **Prolexic Hybrid** combina a potência, a automação e o desempenho do Prolexic On-Prem com a escala e a capacidade líderes do setor do Prolexic Cloud sob demanda para proteger as origens dos clientes contra os maiores ataques DDoS volumétricos.

Levar a segurança além de DDoS

O Akamai Prolexic vem com o Prolexic Network Cloud Firewall, um recurso totalmente de autosserviço e configurável pelo usuário que permite que os clientes definam, implantem e gerenciem facilmente suas próprias listas de controle de acesso (ACLs) e as regras que desejam aplicar na edge da rede. É um firewall na frente de todos os outros firewalls. O Network Cloud Firewall também recomenda ACLs para a melhor postura de defesa proativa com base nos dados de inteligência de ameaças da Akamai e fornece análises acionáveis das regras existentes. Sendo um firewall como serviço de última geração, o Network Cloud Firewall capacita os clientes a:

- Definir defesas proativas para bloquear o tráfego mal-intencionado instantaneamente
- Aliviar a infraestrutura local, movendo as regras para a edge
- Adaptar-se rapidamente às alterações de rede por meio de uma nova interface de usuário

Akamai Edge DNS e **Akamai Shield NS53** protegem e fortalecem a infraestrutura crítica de DNS

O Akamai Edge DNS oferece proteção abrangente contra uma ampla variedade de ataques de DNS em sua infraestrutura de DNS, seja no local, na nuvem ou em ambientes híbridos. A solução também oferece um alto nível de desempenho, resiliência e disponibilidade de DNS. Desenvolvido em uma rede anycast distribuída globalmente, o Edge DNS pode ser implementado como um serviço de DNS primário ou secundário, substituindo ou aumentando a infraestrutura de DNS existente, conforme necessário.

O Akamai Shield NS53 é uma solução de proxy reverso de DNS bidirecional que protege a infraestrutura de DNS local e híbrida, incluindo GSLBs, firewalls e servidores de nomes, contra ataques de esgotamento de recursos de DNS (também conhecidos como NXDOMAIN). Os clientes podem autoconfigurar, administrar, gerenciar e aplicar suas próprias políticas de segurança dinâmicas em tempo real. Consultas ilegítimas de DNS e ataques de inundações de DNS são descartados na edge da rede da Akamai para proteger a infraestrutura crítica de DNS contra ataques DDoS de DNS.

Akamai App & API Protector protege aplicativos e APIs contra ataques DDoS

Reconhecido como uma solução líder de mercado em proteção de APIs e aplicativos da Web (WAAP), o App & API Protector elimina instantaneamente ataques DDoS na camada de rede na edge (para propriedades hospedadas na Akamai Connected Cloud) e fornece estratégias de defesa completas contra ataques DDoS na camada de aplicativo.

Por que a Akamai?

A Akamai oferece as soluções globais de mitigação de DDoS mais confiáveis do mundo. Quer você esteja protegendo aplicativos individuais, data centers inteiros ou a infraestrutura crítica de DNS, a Akamai projetou a mitigação de DDoS com a mais alta capacidade, a maior resiliência e a mais rápida mitigação em mente.

Nós impedimos alguns dos maiores ataques DDoS lançados no mundo. Nossos controles proativos permitem uma verdadeira mitigação desde o primeiro segundo e um SLA líder no setor. Além disso, podemos prestar serviços de proteção contra DDoS para vários clientes e combater vários ataques DDoS de uma só vez.

Como os vetores de ataque DDoS mudam constantemente e os tamanhos dos ataques ficam cada vez maiores, uma plataforma contra DDoS confiável deve inovar, desenvolver e implantar continuamente recursos para detectar ameaças de forma proativa, orquestrar estratégias de mitigação e minimizar os impactos. A Akamai dedica-se a se antecipar às ameaças, impedindo ataques antes que comecem.

Sua estratégia de mitigação de DDoS deve fortalecer sua estratégia híbrida e multinuvem. As soluções de última geração contra DDoS da Akamai protegem sua infraestrutura de rede digital, aplicativos e DNS no local, na nuvem ou em ambos e oferecem as vantagens combinadas de inteligência de máquina e inteligência humana.

Saiba mais

 | Publicado em 10/24