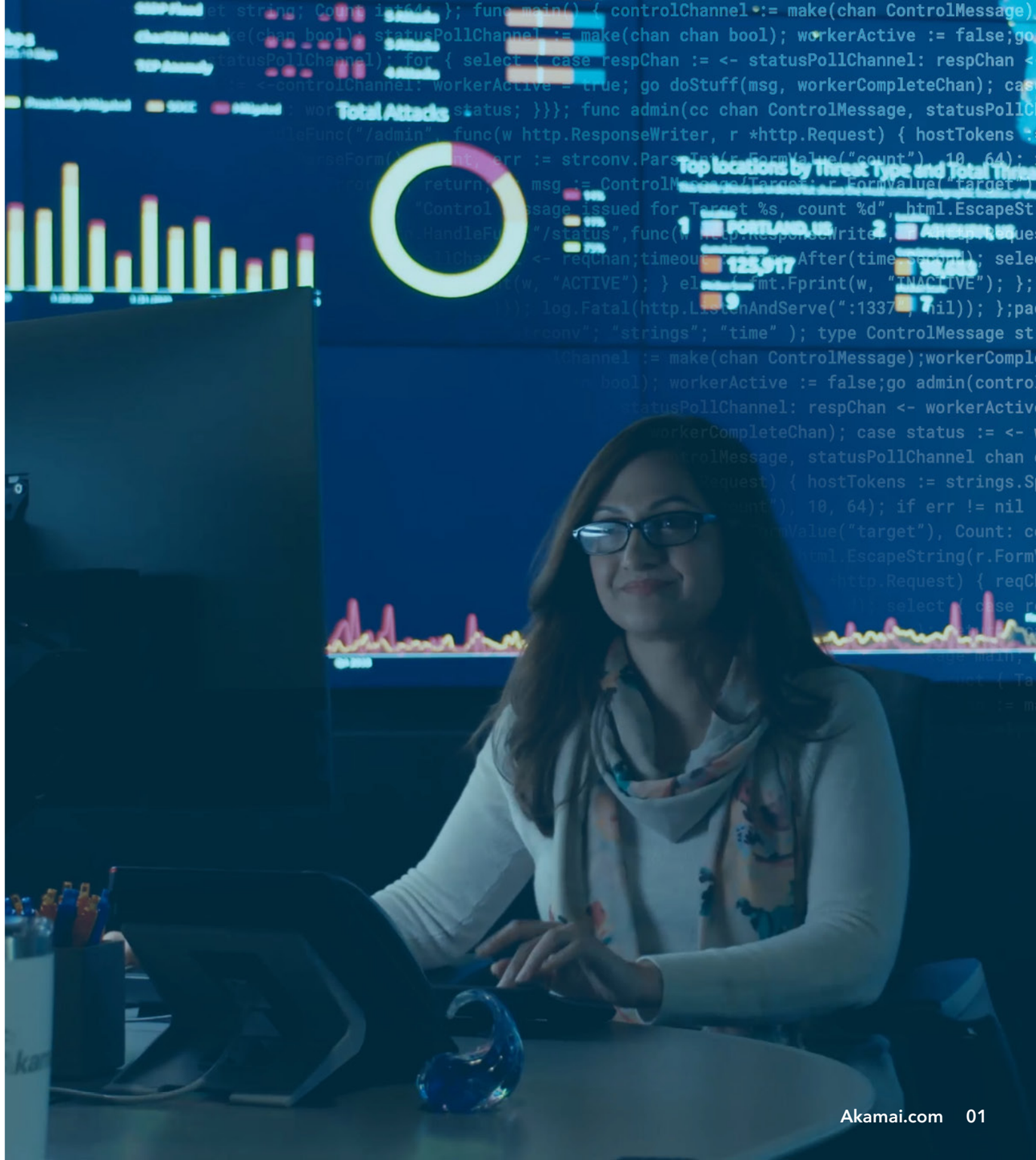
Proteção contra DDoS em um mundo de nuvem híbrida

E-BOOK

Proteção contra DDoS em um mundo de nuvem híbrida

O DDoS (negação de serviço distribuído), um dos tipos mais antigos de ciberameaças, continua sendo um famoso instrumento de interrupção em massa, representando riscos de segurança para praticamente todos os tipos de empresas, de pequeno e grande porte. De fato, de acordo com o IDC, espera-se que os ataques DDoS cresçam a uma taxa de crescimento anual composta (CAGR) de 18% até 2023, um indicador claro de que é hora de aumentar os investimentos em sólidos controles de mitigação. E, embora algumas organizações possam acreditar que sejam alvos de baixo risco para um ataque DDoS, a crescente dependência da conectividade com a Internet para alimentar serviços e aplicações essenciais aos negócios deixará todos expostos ao tempo de inatividade e à redução do desempenho se a infraestrutura não estiver protegida.



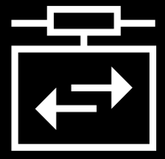
Uma ameaça em **evolução**

O tamanho dos ataques DDoS vem dobrando a cada dois anos, com uma complexidade (o número e a combinação dos vetores de ataque) sem precedentes. Como a disponibilidade de aplicações e da rede é essencial para a continuidade dos negócios, os agentes de ameaças são incentivados a iniciar ataques DDoS volumétricos, de protocolo e na camada de aplicações para interromper qualquer possível ponto de falha, tornando os recursos e ativos voltados à Internet indisponíveis aos usuários finais.

OS INVASORES DE DDoS TÊM COMO ALVO QUALQUER POSSÍVEL PONTO DE FALHA, COMO:

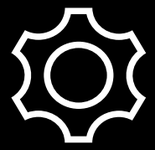
Websites

Aplicações Web e outros serviços empresariais



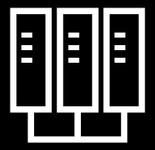
Concentradores de VPN para acesso remoto a recursos corporativos

Controladores SD-WAN



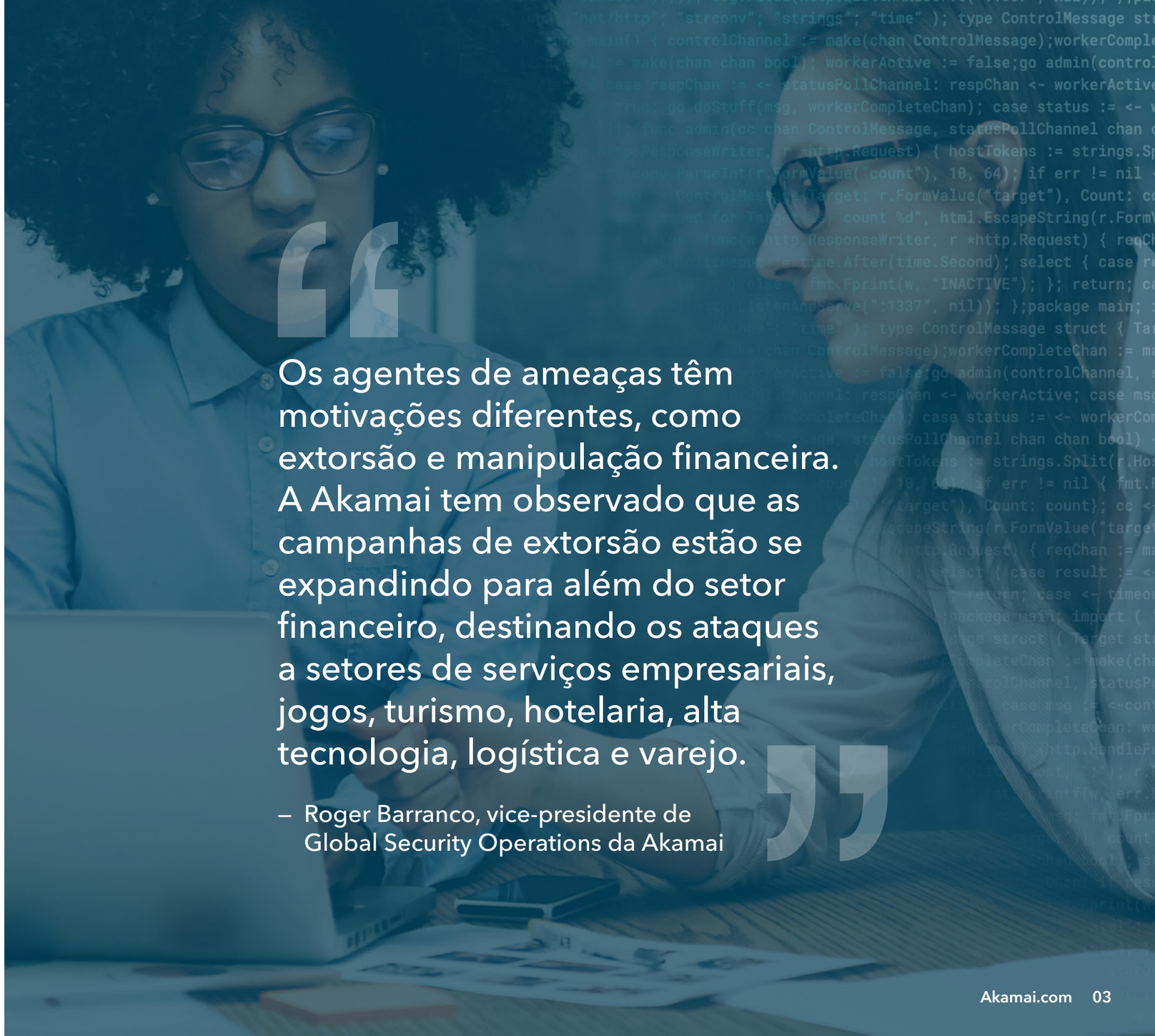
APIs (interfaces de programação de aplicações)

DNS (Sistema de Nomes de Domínio) e servidores de origem



Infraestrutura de rede e data center

Ao realizar o reconhecimento desses ambientes, aplicações e espaços de IP que são vítimas, os invasores podem determinar quais vetores de DDoS causarão o maior dano potencial sobre os serviços voltados à Internet e as infraestruturas de hospedagem de origem. Como a barreira à entrada é insuficiente, esses agentes de ameaças não sofrem com falta de técnicas e ferramentas de ataque (fóruns de ideias, DDoS de aluguel etc.) para ajudar a descobrir pontos fracos ou vulnerabilidades nas defesas das empresas.



> Os agentes de ameaças têm motivações diferentes, como extorsão e manipulação financeira. A Akamai tem observado que as campanhas de extorsão estão se expandindo para além do setor financeiro, destinando os ataques a setores de serviços empresariais, jogos, turismo, hotelaria, alta tecnologia, logística e varejo.
>
> — Roger Barranco, vice-presidente de Global Security Operations da Akamai

As repercussões de um ataque DDoS se intensificam à medida que as organizações trabalham para escalar e proteger os recursos de acesso remoto e garantir a produtividade dos funcionários e os negócios habituais.

As **consequências** de um ataque DDoS

Nos ataques às camadas de rede (camada 3) e transmissão (camada 4), os ataques volumétricos e baseados em protocolo tentam preencher pipes de Internet, sobrecarregar servidores e esgotar entradas de tabelas de estado para tornar as redes e os serviços indisponíveis. Com ataques baseados em aplicações (camada 7), os agentes de ameaças visam a interromper o desempenho da Web e a experiência do usuário por meio de vetores como ataques baixos e lentos e inundações de HTTP para gerar um tempo de inatividade que afeta os resultados financeiros.

Mas as repercussões do tempo de inatividade afetam muito mais que apenas o custo dos serviços visados e a indisponibilidade das aplicações. ***De acordo com o Ponemon Institute, o custo médio anual de um ataque DDoS a uma organização é de US$ 1,7 milhão***, impulsionado pelo aumento do suporte técnico, pelo consumo de recursos de resposta a incidentes, pelas escalações internas, pelos custos de processos judiciais, pela interrupção operacional e pela perda de produtividade dos funcionários.

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

A nuvem continua complicando **as posturas de segurança**

À medida que as organizações desativam os data centers tradicionais e movem aplicações para ambientes hospedados em nuvem, as arquiteturas de segurança se tornam mais complexas. Muitas organizações lutam para manter os ativos voltados à Internet protegidos com o mesmo nível das proteções contra DDoS localizadas no data center. Além da complexidade, muitos IPs hospedados em nuvem ficam fora do controle direto de uma empresa, o que os deixará vulneráveis a um ataque DDoS se não forem devidamente protegidos.

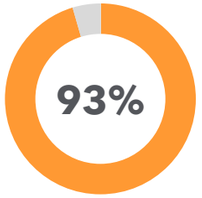
Além disso, os agentes de ameaças estão cientes dessa migração acelerada para instalações de colocalização e para a nuvem pública. Eles estão ansiosos para explorar os pontos fracos da arquitetura e da postura de segurança de uma organização, criados por políticas e requisitos inconsistentes de segurança e pelas dificuldades ao solucionar problemas entre infraestruturas diferentes e fragmentadas hospedadas em nuvem.

A CONCLUSÃO:

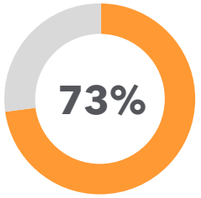
As empresas modernas precisam de proteções adaptáveis para manter protegidos os vários recursos e serviços voltados à Web, independentemente da localização. E, como mais de 93% das empresas (com menos de mil funcionários) utilizam uma estratégia multinuvem, chegou a hora de fechar as lacunas de proteção geradas pela complexidade da infraestrutura.[1]

[1] *https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020*

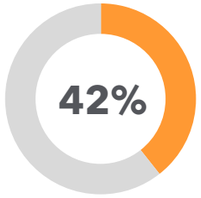
A responsabilidade pela segurança nos ambientes de nuvem pública pode ser inconsistente e variar de provedor para provedor. Muitas organizações fazem falsas suposições que podem deixá-las expostas. Por exemplo, 73% dos entrevistados do setor empresarial em uma pesquisa da IBM acreditam que os CSPs (provedores 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 controle sobre a responsabilidade pela segurança pode gerar comprometimentos: um risco que nenhuma organização deveria estar disposta a aceitar.



das empresas utilizam uma estratégia multinuvem

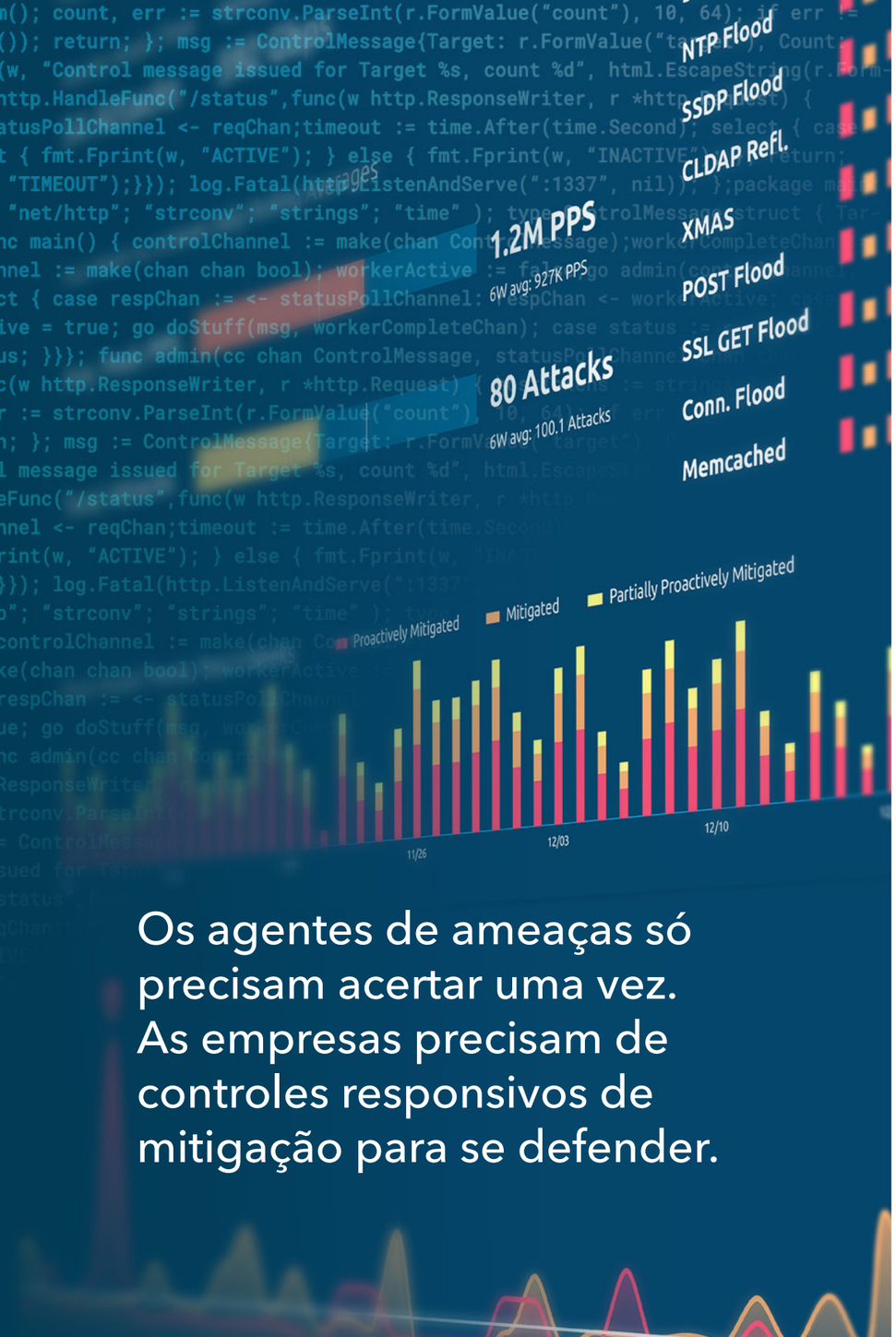


dos entrevistados da pesquisa acreditam que os CSPs de nuvem pública são responsáveis por proteger o SaaS



dos entrevistados acreditam que os CSPs são responsáveis por proteger a IaaS em nuvem

Em um artigo recente, a Forrester observou que a maioria das organizações está escolhendo uma abordagem de estratégia híbrida, utilizando vários provedores de nuvem pública e hospedando cargas de trabalho no local. Assim, a empresa de análise recomenda escolher um provedor de mitigação de DDoS que possa permitir a proteção em arquiteturas híbridas.



As estratégias de mitigação de DDoS **não são todas iguais**

À medida que os investimentos em infraestrutura em nuvem continuam, as equipes de segurança continuam sendo desafiadas a garantir controles consistentes que abrangem os ambientes híbridos. E, já que fica mais difícil proteger as aplicações implantadas em várias infraestruturas em nuvem de back-end, muitas organizações desejam um ponto único de controle para organizar as proteções. Como o conjunto de tecnologia de segurança fica cada vez mais complexo, muitas organizações também desejam um painel de controle único, não só para ter mais visibilidade, mas também para simplificar os relatórios que podem ser alimentados por meio de APIs nos sistemas de correlação de dados de eventos.

Para resolver esse problema, as organizações estão recorrendo aos provedores de segurança de DDoS baseados em nuvem que podem ativar, e não inibir, suas estratégias de migração à nuvem híbrida. Elas querem proteções escaláveis e responsivas, independentemente da localização dos serviços empresariais. Isso é uma resposta direta ao aumento da complexidade operacional necessária para integrar, implantar e gerenciar as proteções contra DDoS no ambiente exclusivo de um CSP. E, como muitos ativos voltados à Internet estão localizados em várias nuvens, a complexidade surge rapidamente.

Além da pressão, muitas soluções internas de mitigação de DDoS dos CSPs ficam para trás em áreas principais: visibilidade, SLAs e geração de relatórios, que são essenciais para capacitar os atuais defensores empresariais.

Para as equipes de segurança, tudo se resume à visibilidade e à 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 muitos chamam os CSPs de a caixa preta da analítica e da geração de relatórios.

Além disso, alguns CSPs não oferecem um SLA de tempo de mitigação e, em vez disso, oferecem créditos de serviço à organização afetada. 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.

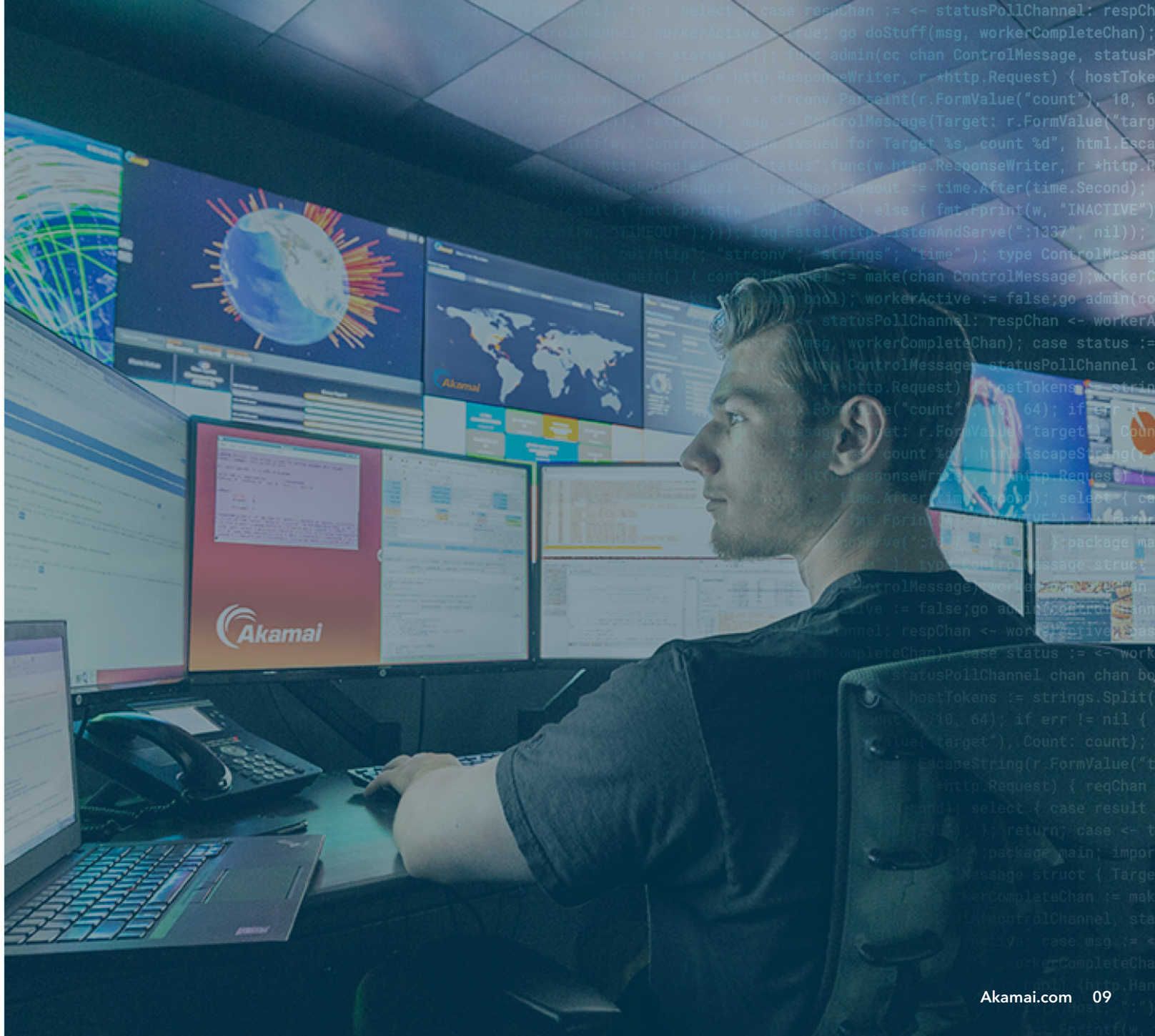
E, finalmente, muitos CSPs não oferecem acesso sob demanda ao suporte do SOC (Centro de operações de segurança) global, que trabalha 24 por dia, 7 dias por semana, além da assistência antes, durante e após os ataques que é padrão entre os principais provedores de mitigação de DDoS baseados em nuvem. E, quando oferecem, isso tem um preço muitas vezes mais caro que uma solução especializada de mitigação de DDoS de um dos melhores provedores do setor. Com uma solução de proteção contra DDoS 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.

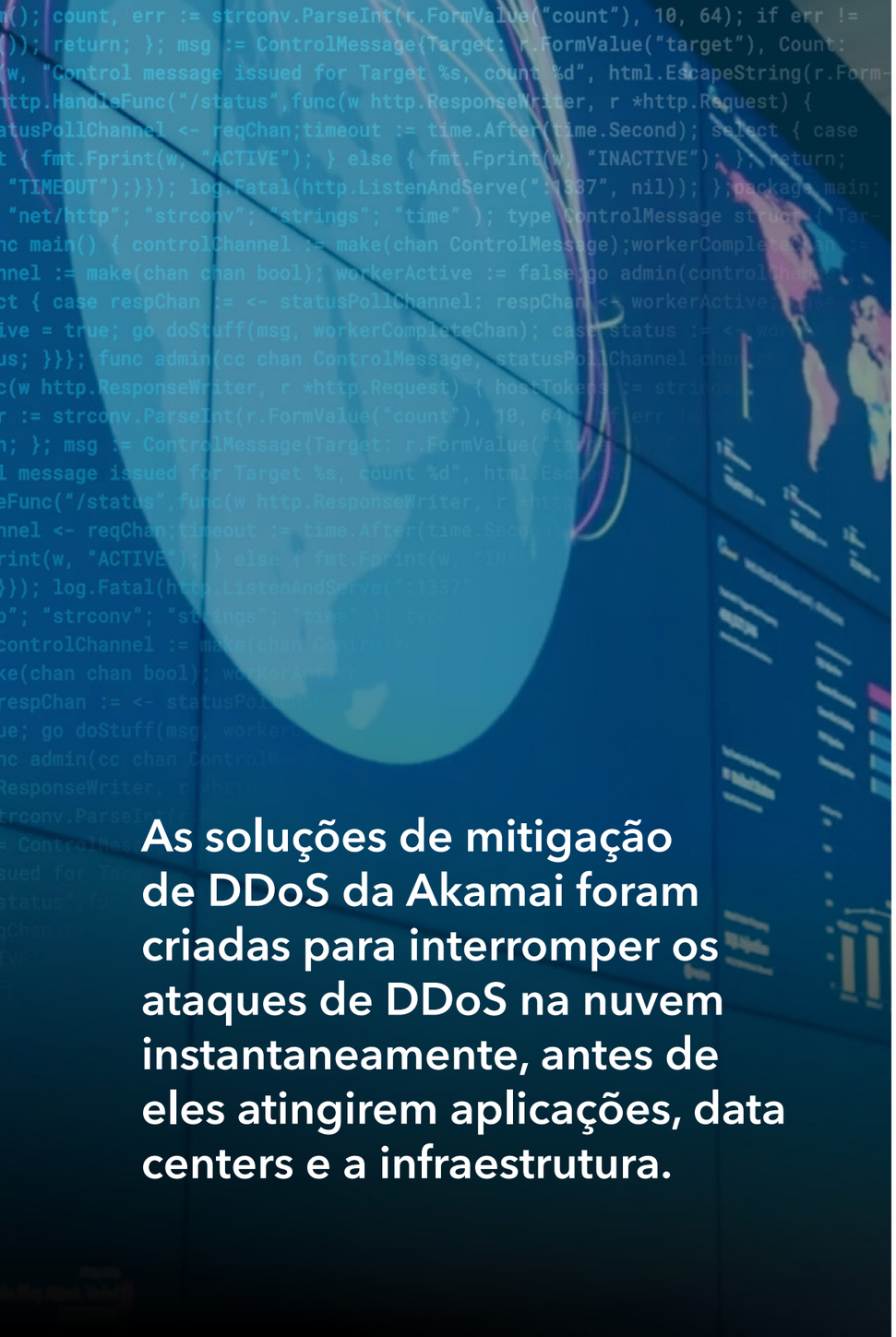
No atual ambiente de ameaças, as empresas modernas estão recorrendo a parceiros de mitigação de DDoS que proporcionam uma experiência de segurança simplificada em ambientes híbridos, ao mesmo tempo que reduzem a complexidade das superfícies de ataque.

Um parceiro de mitigação de DDoS deve ser um viabilizador da estratégia de nuvem, e não um obstáculo, para ajudar a aliviar a pressão sobre a segurança.

Mitigação de DDoS **personalizada** com a Akamai

Assim como as organizações precisam de uma estratégia de nuvem completa, elas também precisam considerar a proteção completa contra DDoS. Ao adotar uma abordagem abrangente, a Akamai atua como a primeira linha de defesa, oferecendo proteção com estratégias dedicadas de mitigação em nuvem, edge e DNS distribuído projetadas para evitar danos colaterais e pontos únicos de falha. Ao contrário de outras arquiteturas de provedores de segurança em nuvem (criadas como uma solução única para todas as situações), as nuvens personalizadas contra DDoS da Akamai oferecem maior resiliência, capacidade dedicada de depuração e maior qualidade de mitigação, tudo ajustado aos requisitos específicos das aplicações Web ou dos serviços baseados na Internet.





As soluções de mitigação de DDoS da Akamai foram criadas para interromper os ataques de DDoS na nuvem instantaneamente, antes de eles atingirem aplicações, data centers e a infraestrutura.

PROTEÇÃO DA EDGE

A edge da Akamai (CDN) entrega e acelera o tráfego da Web usando protocolos HTTP e HTTPS. Cada servidor de edge da Akamai opera como um proxy reverso, encaminhando o tráfego HTTP/S legítimo nas portas 80 e 443 e descartando todos os outros tipos de tráfego na edge da rede. Isso significa que, de forma inerente, todos os clientes da Akamai obtêm a mitigação instantânea de todos os ataques DDoS na camada da rede, integrada à sua entrega na Web.

PROTEÇÃO DO DNS

A mesma tecnologia se aplica ao serviço de DNS autorizado, o Edge DNS, que descarta instantaneamente todo o tráfego que não está na porta 53. Ao contrário das outras soluções de DNS, a Akamai projetou o Edge DNS especificamente para proporcionar disponibilidade e resiliência contra ataques de DDoS, além de desempenho, com redundâncias arquitetônicas em vários níveis, incluindo servidores de nome, pontos de presença, redes e, até mesmo, nuvens IP Anycast segmentadas.

PROTEÇÃO DE DEPURAÇÃO EM NUVEM

Como um serviço de depuração em nuvem testado em batalha, o Prolexic protege data centers inteiros e a infraestrutura voltada à Internet contra ataques DDoS, em todas as portas e protocolos. Ao rotear o tráfego legítimo e mal-intencionado pelo Prolexic, podemos criar modelos de segurança positivos e negativos que impedem de forma proativa e instantânea os ataques DDoS com alta precisão. Os especialistas do SOCC (Centro de comando de operações de segurança) da Akamai atuam como uma extensão da equipe de resposta a incidentes de um cliente para equilibrar a detecção e a resposta automatizadas com a interação humana.

Por que a Akamai

A Akamai tem as maiores e mais maduras nuvens globais de mitigação de DDoS do mundo. Quer você esteja protegendo aplicações individuais, data centers inteiros ou o DNS autorizado, 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 de mitigação permitem uma verdadeira mitigação desde o primeiro segundo, o que é um SLA (Acordo de Nível de Serviço) líder no setor. Além disso, podemos prestar serviços de proteção contra DDoS para vários clientes e combater vários ataques DDoS de uma só vez.

Akamai

Como os vetores de ataques DDoS continuam mudando e os tamanhos dos ataques continuam aumentando, um provedor deve investir continuamente, desenvolver e implantar ferramentas e regras para detectar, organizar e impedir ataques. A Akamai se dedica a se antecipar às ameaças, impedindo ataques antes de eles começarem.

Sua estratégia de mitigação de DDoS deve capacitar sua estratégia de nuvem. A Akamai Intelligent Edge Platform oferece proteções contra DDoS para fazer isso, ajudando os clientes a ampliar a proteção do núcleo à nuvem e à edge, minimizando os riscos e, ao mesmo tempo, oferecendo flexibilidade em relação às futuras evoluções das estratégias de nuvem.

Fale conosco e veja como podemos **proteger** sua empresa

Saiba mais

*A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A plataforma de borda inteligente da Akamai cerca tudo, da empresa à nuvem, para que os clientes e seus negócios possam ser rápidos, inteligentes e protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a alcançar a vantagem competitiva por meio de soluções ágeis que estendem a potência de suas arquiteturas multinuvem. A Akamai mantém as decisões, os apps e as experiências mais próximos dos usuários, e os ataques e as ameaças cada vez mais distantes. O portfólio de soluções de segurança de borda, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeo da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, sete dias por semana, durante todo o ano. Para saber por que as principais marcas mundiais confiam na Akamai, visite **www.akamai.com**, **blogs.akamai.com** ou **@Akamai** no Twitter. Nossas informações de contato globais podem ser encontradas em **www.akamai.com/locations**. Publicado em 11/20.*