Akamai

WHITE PAPER

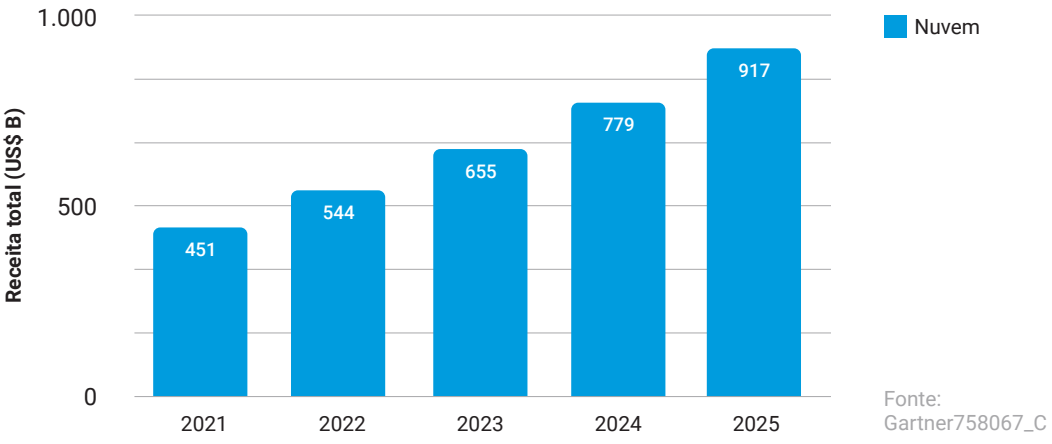
Abrindo o caminho para a microssegmentação

Um guia de estratégia para implementar a microssegmentação em nuvens híbridas

Mais nuvens na previsão

A migração de grandes quantidades de dados e processamento de dados para a nuvem, ou mais precisamente, para várias nuvens, é provavelmente a maior mudança na computação empresarial na última década. Mais organizações estão migrando para nuvens públicas e, normalmente, para arquiteturas de data center públicas-privadas híbridas. Ao mesmo tempo, elas estão aproveitando a infraestrutura como um serviço (IaaS) na busca de uma agilidade cada vez maior. A Gartner, analista de tecnologia, projeta que até 2025, pouco mais da metade de todos os gastos de TI em segmentos de mercado endereçáveis terão mudado de soluções tradicionais para a nuvem pública, em comparação com 41% em 2022, e espera-se que os gastos totais com receita na nuvem pública excedam US$ 900 bilhões até 2025.[1]

A distinção entre "a nuvem" e "múltiplas nuvens" não é trivial. Cada vez mais, as empresas estão adotando plataformas multinuvem e provedores de serviços. Uma coisa é clara: A ideia de um data center empresarial como um espaço físico único e seguro está se extinguindo como os dinossauros. Os data centers modernos são cada vez mais uma mistura heterogênea de ambientes e tecnologias que combinam servidores físicos, máquinas virtuais e contêineres em instalações locais, nuvens privadas e provedores de IaaS de nuvem pública. E essas instalações diferentes não são estáticas – as organizações estão constantemente mudando dados e cargas de trabalho entre seus vários ambientes locais e em nuvem conforme os níveis de tráfego e as demandas de processamento exigirem.



Previsão de receita mundial de serviços de nuvem pública (em bilhões)

O aumento da complexidade gera novas vulnerabilidades e amplia as superfícies de ataque

Os clientes de nuvem certamente se beneficiam da agilidade, elasticidade e escalabilidade adicionais que a IaaS oferece a eles. Esses benefícios são uma grande parte do que torna a nuvem tão atraente. As compensações para isso, no entanto, são uma complexidade de gerenciamento muito maior, uma perda de visibilidade da carga de trabalho entre os ambientes e, por sua vez, um cenário de segurança cibernética inexplorado. Trabalhar com vários provedores de nuvem significa que as equipes de segurança precisam lidar com padrões e recursos de segurança amplamente variados. As ferramentas de segurança tradicionais projetadas para servidores e endpoints locais simplesmente não conseguem lidar com a escala e a complexidade da nuvem. As ferramentas mais recentes fornecidas pelos fornecedores de IaaS podem ser eficazes no ambiente do provedor, mas têm pouco valor em uma infraestrutura de vários provedores.

Além disso, mesmo nessa era de virtualização e "tudo definido por software", a mentalidade de segurança (e, portanto, a maior parte do investimento) ainda está fundamentada na necessidade percebida de bloquear ataques especificamente no ponto de entrada. Isso não quer dizer que as defesas de perímetro devam ser derrubadas – elas ainda são muito relevantes para a pilha de segurança de TI – mas não funcionam tão bem quando o perímetro está em constante mudança. Os dados e as cargas de trabalho estão indo e voltando entre nuvens públicas e privadas e data centers locais, e os usuários que os acessam estão trabalhando cada vez mais em locais remotos que podem ou não ter os controles de segurança apropriados em vigor.

O grande número de violações de dados relatadas todos os anos é suficiente para nos dizer que invasores astutos estão passando por defesas de perímetro praticamente à vontade. E, uma vez lá dentro, eles encontram uma rede relativamente plana onde os ativos que residem dentro do perímetro estão praticamente desprotegidos. Apesar de toda a flexibilidade que as organizações ganharam, a complexidade adicional de gerenciar e proteger infraestruturas multinuvem multiplicou exponencialmente a superfície de ataque; com pouco ou nenhum controle de comunicação implementado, cada servidor individual torna-se uma superfície de ataque por si só. Como resultado, os invasores podem passar mais tempo se movendo lateralmente — e sem serem detectados — entre cargas de trabalho de tráfego leste-oeste para encontrar seus ativos mais críticos.

A segmentação de rede é uma prática de segurança bem compreendida e estabelecida, mas hoje em dia pode ser difícil de executar em infraestruturas de TI dinâmicas e em escala de nuvem, onde as cargas de trabalho estão se comunicando e muitas vezes migrando entre segmentos. Os clientes de nuvem corporativa perceberam que precisam segmentar ainda mais suas aplicações e cargas de trabalho para controlar rigidamente os fluxos de comunicação em tempo real e detectar e impedir ameaças no data center antes que possam causar qualquer dano. O que é necessário é uma solução que reduza a complexidade da segurança trabalhando consistentemente nos limites da infraestrutura para reduzir a superfície geral de ataque, permitindo que as equipes de segurança detectem mais ameaças com mais rapidez e limitem sua propagação.

É aí que entra a microssegmentação.

Microssegmentação definida

A Gartner define a microssegmentação como "o processo de implementação do isolamento e da segmentação para fins de segurança no datacenter virtual". Além disso, a microssegmentação "reduz o risco de uma disseminação lateral de ataques avançados em data centers corporativos e permite que as empresas apliquem políticas de segmentação consistentes em cargas de trabalho locais e baseadas em nuvem."[2]

A microssegmentação geralmente funciona estabelecendo políticas de segurança em torno de aplicações individuais ou grupos de aplicações, independentemente de onde elas residem no data center híbrido. Essas políticas determinam quais aplicações e componentes podem ou não se comunicar entre si. Assim, qualquer tentativa de comunicação não autorizada é um indicador instantâneo de uma ameaça. Na melhor das hipóteses, as tecnologias de microssegmentação são independentes da infraestrutura, de modo que as políticas de segurança podem continuar a proteger suas respectivas aplicações à medida que se movem entre os ambientes de nuvem.

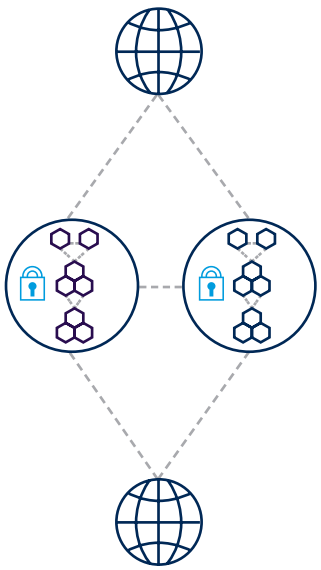
Áreas de solução para segmentação

Segmentação da infraestrutura

Proteger o tráfego de aplicações em uma infraestrutura específica.

Segmentação de aplicações

Proteger o tráfego entre aplicações e redes externas.



Microssegmentação

Regras que protegem o tráfego dentro de aplicações com contexto adicional, como atribuição no nível do processo.

2 Gartner, "Technology Insight for Microsegmentation (insight de tecnologia para microssegmentação)", março de 2017; "Hype Cycle for Cloud Security 2017 (ciclo de hype para segurança na nuvem 2017)", julho de 2017"

O caso da microssegmentação

Os data centers dinâmicos de hoje exigem que as empresas mudem sua atenção da prevenção de invasões e do gerenciamento de acesso para as próprias cargas de trabalho e aplicações. E isso parece estar acontecendo em um ritmo acelerado. Mesmo em 2017, a Gartner começou a perceber uma tendência de "maior foco na proteção da carga de trabalho do servidor contra ameaças direcionadas avançadas que ignoram o perímetro tradicional e a proteção baseada em assinatura. Normalmente, esses ataques são motivados financeiramente e têm como alvo cargas de trabalho de servidores e aplicações como forma de obter dados ou transações confidenciais."[3]

Um dos principais impulsionadores da microssegmentação é a necessidade de proteger aplicações e cargas de trabalho essenciais. Isso pode parecer apenas uma questão de interesse próprio ou de boa prática comercial, mas, em muitos casos, também é exigido por políticas de segurança e requisitos regulatórios.

As equipes de segurança precisam encontrar maneiras de reduzir a superfície de ataque em expansão nos data centers, o que significa reduzir a vulnerabilidade dos servidores que executam aplicações. As técnicas de autenticação tradicionais, como bloqueio de assinaturas ou permissão de aplicações, são subvertidas com muita facilidade por invasores sofisticados. A microssegmentação permite que as equipes definam e apliquem políticas rígidas e granulares de acesso e comunicação. Ela também deve melhorar a visibilidade dos fluxos de aplicações e permitir que as equipes avaliem melhor sua postura de segurança.

Você precisa de microssegmentação?

Responder a algumas perguntas simples ajudará você a determinar sua necessidade de microssegmentação.

- Você está em um setor regulamentado ou precisa cumprir as normas que regem a segurança de dados e transações?
- Você tem uma infraestrutura híbrida com cargas de trabalho que abrangem várias nuvens?
- Você está executando aplicações em máquinas virtuais ou contêineres?
- Você sente uma perda de visibilidade e controle das cargas de trabalho?
- Você pode dizer, a qualquer momento, que uma ameaça está presente ou que um ataque está em andamento em seu data center?
- Você pode controlar a segurança em toda a sua infraestrutura por meio de um "painel único"?

Os quatro principais obstáculos no caminho

Se os especialistas em segurança geralmente concordam com a necessidade de microssegmentação nos data centers dinâmicos atuais, por que é considerado tão assustador implementar com eficiência e sucesso? As organizações que tentam implementar a microssegmentação usando ferramentas convencionais geralmente encontram quatro grandes obstáculos:

1. **Falta de visibilidade no nível do processo**
   Este é provavelmente o primeiro obstáculo que você encontrará - você não pode proteger o que não pode ver. A microssegmentação tem a ver com a proteção individual e de grupos de aplicações e processos de fluxo de trabalho. As equipes de segurança precisam de visibilidade dos fluxos de tráfego leste-oeste reais para compreendê-los no contexto. A maioria das ferramentas não oferece essa profundidade.

2. **A falta de suporte a multinuvem híbrida**
   As políticas de segurança de microssegmentação precisam ser capazes de dimensionar facilmente em ambientes locais e de nuvem pública, e seguir as cargas de trabalho à medida que elas se movem de um ambiente a outro. As ferramentas projetadas para funcionar em um ambiente específico são ineficazes em ambientes híbridos.

3. **Mecanismos de política inflexíveis**
   Como observado anteriormente, os data centers atuais não são estáticos. As medidas de segurança também não podem ser: a mentalidade de "definir e esquecer" não funcionará mais. Infelizmente, as ferramentas existentes dos provedores de nuvem não permitem a flexibilidade necessária para dimensionar, testar e refinar regras constantemente. Esse desafio é composto por infraestruturas híbridas que exigem várias ferramentas de políticas.

4. **Nenhuma integração com controles complementares**
   Feita corretamente, a microssegmentação não é apenas para proteger processos, mas também para capturar ataques. No entanto, as ferramentas de microssegmentação de função única geralmente não incluem recursos de detecção de violação, deixando para o usuário integrar as ferramentas e fazê-las funcionar juntas de maneira eficaz. Essa abordagem de colcha de retalhos traz um alto risco de falha.

Projetos malsucedidos são a norma, não a exceção

Devido a esses obstáculos, não surpreende que a maioria dos projetos de microssegmentação tende a sofrer ciclos de implementação glaciais e podem aumentar os custos, os recursos fiscais e, por fim, não atingir seus objetivos. As organizações frequentemente precisam tentar adivinhar o que precisa ser segmentado (devido à falta de visibilidade) e decidir quanta segmentação é necessária. Elas podem passar meses criando planilhas de regras complexas para comunicações no nível do processo, incapazes de reconhecer oportunidades para agrupar aplicações e simplificar políticas. Muitas vezes, eles erram na lateral da "supersegmentação", definindo muitas políticas discretas, resultando em muita complexidade de segurança, o que é precisamente o que você está tentando superar. Como a Gartner observou, "... mais de 70% dos projetos de segmentação terão seu projeto inicial reprojetado devido à supersegmentação."[4]

A supersegmentação corre o risco de desacelerar as aplicações e, por fim, os negócios. Mas o pêndulo pode pesar muito para o outro lado, em direção a uma segmentação insuficiente, e acabar comprometendo sua postura de segurança.

Estratégia para uma jornada bem-sucedida de microssegmentação

O caminho para a implementação da microssegmentação não é uma linha reta - há muitas voltas e reviravoltas conforme você descobre, entende e controla os fluxos de comunicação em seu ambiente. As equipes de segurança precisam de flexibilidade ao desenvolver políticas de segurança para incorporar constantemente novas alterações ou adições sem quebrar aplicações. Muitas soluções oferecem mecanismos inflexíveis de criação de políticas, forçando as equipes de segurança a implementar regras incompletas ou ineficazes antes de estarem prontas.

Simplesmente, uma implementação bem-sucedida é aquela que supera ou contorna os quatro principais obstáculos, evitando complexidade indevida e reduzindo o risco de sub ou super segmentação, permitindo uma abordagem em fases. Isso significa ter uma solução que atenda a esses requisitos:

- **Visibilidade no nível do processo:** as equipes precisam ter a capacidade de revelar, coletar e normalizar todos os fluxos leste-oeste e norte-sul; ferramentas que permitem a descoberta automática de aplicações e uma compreensão de seus requisitos de comunicação; e a capacidade de filtrar vários atributos de aplicações para facilitar a rotulagem e o agrupamento de ativos que podem compartilhar políticas.

- **Um mecanismo de política flexível:** você deve ser capaz de projetar simultaneamente práticas recomendadas de alto nível e regras de conformidade para grandes segmentos e regras mais granulares para microssegmentos. A solução deve permitir que você passe gradualmente de alerta para aplicação. E isso deve permitir que você estabeleça políticas que possam funcionar em todas as plataformas, dispositivos e nuvens.

- **Implantação, manutenção e gerenciamento de alterações simplificados:** o sistema deve facilitar a implantação, a manutenção e a modificação de regras conforme necessário. Ele deve incorporar recursos integrados de detecção de violação e resposta a incidentes. Por fim, suas políticas devem ser suficientemente bem definidas para que você possa integrá-las a ferramentas de implantação automatizada (CI/CD) para cada nova aplicação iniciada.

Recursos de solução ideais

É claro que existem muitas ferramentas de microssegmentação no mercado, e nem todas elas facilitam esse caminho. Para garantir uma implementação mais simples e bem-sucedida, certifique-se de escolher uma solução com estes recursos:

- **Descoberta automática de aplicações**, com visibilidade completa no nível do processo para servidores bare-metal, máquinas virtuais e contêineres

- A capacidade de definir **consultas robustas e extensas** para criar rótulos contextuais e grupos de objetos

- Um **mecanismo de políticas flexível** com design de regras inteligente que ajuda você a refinar, fortalecer e manter políticas

- Um **recurso integrado de detecção de violação de vários métodos** para encontrar mais ameaças mais rapidamente e limitar sua propagação

- **Suporte à infraestrutura híbrida** – uma plataforma que funciona com qualquer infraestrutura – data centers, nuvens públicas e privadas e muito mais

Uma solução com esses recursos essenciais colocará você no caminho mais bem-sucedido para implementar a microssegmentação, permitirá que você supere os obstáculos e complexidades conhecidos e prepare-se para colher todas as vantagens comerciais de uma infraestrutura de nuvem híbrida flexível sem sacrificar a segurança.

Data centers híbridos, plataformas multinuvem e IaaS oferecem às organizações mais flexibilidade, escalabilidade e agilidade do que seria possível em um data center "fechado" no local. Mas eles também deixam aplicações e cargas de trabalho - os ativos reais que os invasores virtuais estão atacando - mais expostas e vulneráveis. Embora a microssegmentação seja amplamente considerada uma prática recomendada na proteção de cargas de trabalho na nuvem, as empresas estão com dificuldade em acertar. A boa notícia é que você não precisa fazer tudo de uma só vez. As soluções avançadas de hoje, juntamente com uma abordagem gradual, tornam muito mais fácil o caminho para implementar a microssegmentação. E isso significa uma melhor segurança para os ativos mais importantes da sua organização.

Saiba mais sobre a implementação bem-sucedida da microssegmentação em akamai.com/guardicore

1 "Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025 (Gartner diz que mais da metade dos gastos com TI corporativa nos principais segmentos do mercado mudará para a nuvem até 2025)." Gartner, 9 de fevereiro de 2022.

2 Heiser, Jay. "Hype Cycle for Cloud Security, 2017 (Ciclo de hype para segurança na nuvem, 2017)." Gartner, 17 de julho de 2017.

3 MacDonald, Neil. "Market Guide for Cloud Workload Protection Platforms (Guia de mercado para plataformas de proteção de carga de trabalho em nuvem)." Gartner, 22 de março de 2017.

4 Young, Greg. "Best Practices in Network Segmentation for Security (Melhores práticas na segmentação de rede para segurança)." Gartner, 28 de julho de 2016.

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicações e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. Saiba mais sobre as soluções de segurança, computação e entrega da Akamai em akamai.com e akamai.com/blog ou Akamai Technologies no Twitter e LinkedIn. Publicado em 05/23.