WHITE PAPER

Como proteger cargas de trabalho na AWS com segmentação abrangente: segurança mais simples e rápida

Introdução

Não deixe que as preocupações com segurança impeçam a adoção da nuvem. Uma solução pode lidar com visibilidade, prevenção de movimento lateral e detecção e resposta a violações para ativos e recursos na AWS.

Os benefícios de usar recursos da PaaS (plataforma como serviço) na Amazon Web Services (AWS) e migrar cargas de trabalho críticas para fora do local são claros: tira os custos de infraestrutura e a manutenção das suas mãos, melhora a escalabilidade e a elasticidade com recursos e energia quase ilimitados e utiliza as mais recentes inovações, como aprendizado de máquina e IA, para impulsionar o desempenho e a análise. No entanto, as preocupações com a segurança estão limitando muitas empresas, especialmente porque os recursos de nuvem estão entre os principais alvos para ataques cibernéticos.

O desafio da segurança na AWS

Ao considerar um ambiente totalmente novo, não é surpreendente que você precise rever a segurança do zero. Você pode ser um iniciante na nuvem ou pode estar migrando de um fornecedor diferente, escolhendo uma nova solução híbrida ou adicionando a AWS ao seu ecossistema existente. De qualquer forma, a nuvem exige seu próprio conjunto de ferramentas específico para lidar com os desafios exclusivos que essa infraestrutura apresenta. Alguns fatores são comuns para todos os fornecedores de nuvem, enquanto outros são exclusivos do Microsoft Azure, do Google Cloud Platform ou da AWS. Veja abaixo algumas das principais preocupações das empresas que usam nuvem ou nuvem híbrida que incluem a tecnologia AWS.

Compreensão da responsabilidade compartilhada: quando você muda suas cargas de trabalho para a AWS ou quando utiliza seus recursos de PaaS integrados, você precisa reconhecer que ainda tem muita responsabilidade. Você precisará proteger os dados, os aplicativos e as plataformas dos clientes. A falta de entendimento sobre o modelo de responsabilidade compartilhada é o motivo pelo qual a Gartner prevê que 99% das falhas de segurança na nuvem serão culpa do cliente até 2025.

Falta de visibilidade: você não pode controlar aquilo que não pode ver. Na nuvem, a visibilidade é muito mais complicada, especialmente quando se trata de proteger e visualizar o tráfego de rede que se move para leste-oeste e para norte-sul. Observar apenas os fluxos não é suficiente. Seus ativos essenciais podem estar espalhados por várias contas, contêineres ou grupos de segurança de rede da AWS e, sem contextualizar tudo isso, pode ser impossível ter uma noção precisa dos fluxos e interdependências.

Controle limitado para criação de políticas: se sua empresa está acostumada a ter insights na camada 7 no local, você não vai querer dar um passo atrás apenas para a visibilidade da camada 4, perdendo aquele insight granular e controle agora que suas cargas de trabalho estão na nuvem. Os grupos de segurança da Amazon oferecem suporte ao controle de tráfego para a camada 4. Mas com visibilidade e controle da camada 7, independentemente da infraestrutura subjacente, você pode fazer mais do que confiar apenas em portas e IPs, que são insuficientes para detecção de violação ou solução de problemas.

Segurança do contêiner: a AWS usa os grupos de segurança da Amazon para aplicar a política de segurança de contêineres, mas isso é limitado a clusters em vez de pods individuais. Para obter uma visão completa das comunicações, você precisa de uma solução que possa reconhecer o contexto de uma rede de sobreposição em execução no topo e possa detalhar de maneira granular até o nível do pod. Isso fica mais complexo quando você deseja criar políticas de rede que incluam VMs (máquinas virtuais) e contêineres, e geralmente acaba fazendo com que as organizações tenham que lidar com dois conjuntos de controles de segurança.

Adoção de PaaS: há uma tendência significativa de adoção de recursos de PaaS, além de migração de cargas de trabalho críticas para a nuvem, refletindo as necessidades em evolução das organizações centradas na nuvem. No entanto, esses recursos de PaaS não suportam agentes, portanto, a maioria das soluções de segurança baseadas em agentes é muito limitada para estender a proteção total aos recursos de PaaS. Isso pode resultar em uma política de segurança na nuvem fragmentada, criando uma sobrecarga adicional para suas equipes e, possivelmente, deixando lacunas de segurança que podem ser exploradas por agentes de ameaças.

Como combater esses problemas com uma plataforma de segurança multifuncional

A Amazon fornece determinadas ferramentas integradas, como os grupos de segurança da Amazon, que trabalham para combater alguns dos desafios da migração da sua infraestrutura para a nuvem. Incentivamos as organizações a aproveitar ao máximo o IAM (gerenciamento de identidade e acesso) da AWS, usando grupos para atribuir permissões, alternando credenciais regularmente e utilizando grupos de IAM para garantir a simplicidade. No entanto, essas ferramentas são apenas um ponto de partida na nuvem pública dinâmica de hoje, especialmente quando você considera um ambiente híbrido que cobre tudo, desde a infraestrutura legada até a tecnologia de contêiner e recursos de PaaS que estão sendo utilizados em ambientes de nuvem pública diferentes.

Uma solução de segurança sofisticada permitirá que você complemente o que a AWS oferece com uma tecnologia que remove pontos cegos e funciona perfeitamente com o restante da sua pilha de segurança, mesmo em um ambiente híbrido. Veja o que a Akamai oferece.

Visibilidade total das instâncias da AWS

Quanto mais complexa for a infraestrutura de TI, mais importante será ter uma visibilidade profunda e automatizada. Movimentos, adições, alterações e exclusões manuais não são apenas não confiáveis e propensas a falhas e erros, elas são uma desaceleração e, portanto, uma barreira para a adoção da nuvem. Em contraste, a visibilidade aprimorada e automatizada descobrirá todos os aplicativos e fluxos, adicionando visibilidade às suas instâncias até o nível de processo individual.

O Akamai Guardicore Segmentation, a principal oferta da Plataforma Akamai Guardicore para Zero Trust, inclui uma poderosa API da AWS que extrai dados de orquestração com um componente dedicado para coletar informações de ativos, fluxos e tags, oferecendo um contexto valioso que você pode usar para rotulagem e mapeamento de aplicativos. À medida que você usa sua infraestrutura como base, você tem os detalhes necessários para entender totalmente como seus aplicativos se comunicam uns com os outros, onde estão as interdependências e como a política deve ser criada para permitir fluidez e agilidade. Em vez de ter uma solução de segurança separada para cada fornecedor ou ambiente de nuvem, os usuários podem visualizar informações nativas da nuvem e dados específicos da AWS, tudo no mesmo painel. Nossa solução funciona em plataformas, infraestruturas e nuvens, para que você possa ter a garantia de zero ponto cego.

Segmentação e aplicação: uma política que segue a carga de trabalho

Depois de obter essa visão de "painel único" de todos os seus ambientes, você pode começar a projetar e implantar a política de segurança. A política de reconhecimento de aplicativos vai além do que os grupos de segurança da Amazon podem alcançar, fornecendo a granularidade de camada 7 (em vez da granularidade da camada 4). Embora algumas organizações estejam tentando usar firewalls de última geração no local para limitar o movimento lateral, isso só oferece suporte à segmentação superficial do tráfego leste-oeste. É proibitivamente difícil como uma solução para controles de segmentação granular devido à necessidade de grandes mudanças de infraestrutura e rede para redirecionar o tráfego através do firewall. Mesmo que fosse uma opção local, ela também deixa as organizações com o problema de manter esse nível de controle na nuvem.

A microssegmentação da camada 7 é a resposta, com políticas criadas para cargas de trabalho dinâmicas, sem a necessidade de mudar a infraestrutura de rede subjacente. À medida que a política segue a própria carga de trabalho, removemos a necessidade de mudanças manuais e aprimoramos a capacidade da sua organização de adotar a agilidade e processos de DevOps em rápida evolução. Uma política de microssegmentação pode simplificar um ambiente híbrido impondo regras entre regiões, VPCs, contêineres, VMs e no local, tudo com uma expressão de política consistente. Começando com a visibilidade que fornecemos, você pode definir e aplicar políticas de segmentação em poucos minutos. Seu processo de criação de políticas também é aprimorado por recomendações de políticas automáticas que fornecem os melhores protocolos de segurança da categoria na nuvem pública.

Detecção de violações e resposta a incidentes na nuvem da AWS

Com a Akamai, você pode levar sua segurança da AWS além da segmentação ou visibilidade apenas. A detecção de violações de políticas é uma parte importante da detecção de violações, permitindo que você responda a uma possível ciberameaça em tempo real, com detalhes no nível do aplicativo. Oferecemos vários métodos de detecção de violações que podem alertar você imediatamente sobre uma intenção maliciosa em um ambiente de nuvem híbrida.

- **Análise de reputação:** detecte automaticamente informações suspeitas nos fluxos, de nomes de domínio e endereços IP a hashes de arquivos e linhas de comando
- **Fraude dinâmica:** envolva os invasores sem o conhecimento deles, desviando-os para um ambiente de honeypot de alta interação, onde você pode aprender com segurança com o comportamento deles
- **Ferramentas para acelerar a resposta a incidentes:** faça a integração com a AWS para permitir que quaisquer violações de políticas ou incidentes de segurança sejam enviados em tempo real para o AWS Security Hub
- **Busca personalizada de ameaças:** aproveite a infraestrutura e a enorme inteligência global de ameaças da Akamai para interromper as ameaças mais evasivas no seu ambiente de nuvem híbrida com o nosso serviço Akamai Hunt

Juntando tudo isso para aumentar a segurança na AWS e além

Colher os benefícios da nuvem pública não significa necessariamente se contentar com menos segurança, visibilidade ou controle do que sua organização aproveita no local. Com a Akamai, você pode obter visibilidade completa de seus ativos da AWS e recursos em toda a sua infraestrutura. Usando esse mapa de base, simplificamos a criação de políticas e aprimoramos as medidas de segurança atuais para fornecer controle granular sem a necessidade de suporte manual. Os complementos da detecção de violações e resposta a incidentes fornecem uma solução de segurança completa que cobre todas as suas bases na nuvem AWS e além disso.

Acesse akamai.com/guardicore para obter mais informações.

Sobre as soluções de segurança da Akamai

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e LinkedIn. Publicado em 11/24.