Akamai

WHITE PAPER

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

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 na AWS.

Mais de 60% das empresas em todo o mundo citam a segurança como um dos principais motivos para evitar a adoção da nuvem. Os benefícios de mover cargas de trabalho essenciais para a AWS são claros, tirando os custos de infraestrutura e a manutenção de suas mãos, melhorando a escalabilidade e a elasticidade com recursos e energia quase ilimitados e utilizando as mais recentes inovações, como aprendizado de máquina e IA, para aumentar o desempenho e a análise. No entanto, as preocupações com a segurança estão limitando muitas empresas.

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 requer seu próprio conjunto de ferramentas específico, lidando com os desafios únicos que essa infraestrutura apresenta. Alguns fatores são comuns para todos os fornecedores de nuvem, enquanto outros são exclusivos do Azure, do GCP (Google Cloud Platform) ou da AWS. Estas são 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, você precisa reconhecer que ainda tem muita responsabilidade. Você precisará proteger os dados, as aplicações 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 er 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 reconheça 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 e contêineres, geralmente resultando em organizações que lidam com dois conjuntos de controles de segurança.

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 (Identity and Access Management) da AWS, usando grupos para atribuir permissões, atualizando 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 multinuvem e contêiner. 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 Guardicore Segmentation oferece:

Visibilidade total das instâncias da AWS

Quanto mais complexa for a infraestrutura de TI, mais importante será ter uma visibilidade profunda e automatizada. Mudanças manuais, adições, alterações e exclusões 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 todas as aplicações e fluxos, adicionando visibilidade às suas instâncias até o nível de processo individual.

A Akamai Guardicore Segmentation inclui uma API poderosa da AWS que extrai dados de orquestração, oferecendo um contexto valioso que você pode usar para rotulagem e mapeamento de aplicações, puxando automaticamente tags EC2 para visualizar instâncias EC2. À medida que você usa sua infraestrutura como base, você tem os detalhes necessários para entender totalmente como suas aplicações se comunicam

umas com as outras, 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 pontos cegos.

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 aplicações vai além do que os grupos de segurança da Amazon podem alcançar, fornecendo a 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 suporta a segmentação grosseira 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 o DevOps em rápida evolução. Simplificando um ambiente híbrido, uma política de microssegmentação pode impor 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

A escolha de uma solução de serviço completo como a Akamai Guardicore Segmentation permite que você leve sua segurança da AWS além da segmentação ou da visibilidade apenas. A detecção de violações de políticas é uma parte importante da detecção de violações, permitindo que você responda a uma possível ameaça cibernética em tempo real, com detalhes no nível da aplicação. Oferecemos vários métodos de detecção de violações que podem alertar 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:** a integração com a AWS permite 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 da Akamai Guardicore Segmentation 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

Uma mudança para a nuvem não significa necessariamente se contentar com menos segurança, visibilidade ou controle do que sua organização desfruta no local. Com a Akamai Guardicore Segmentation, você pode obter visibilidade completa de suas instâncias da AWS junto com toda a sua infraestrutura. Usando esse mapa fundamental, a criação de políticas é contínua e aprimora os grupos de segurança da AWS para fornecer controle granular sem a necessidade de suporte manual. Complementada pela detecção de violações e resposta a incidentes, você tem uma plataforma completa que cobre todas as suas bases na nuvem AWS.

Acesse akamai.com/guardicore para obter mais informações.