Guardicore

# Questões de Segurança da AWS Cloud Que Você Não Deve Ignorar

De acordo com a Gartner, até 2022, **95% das falhas de segurança nas nuvens serão culpa do cliente**. **Usar a nuvem com AWS** significa construir uma estratégia de segurança de nuvem que enfrente os desafios diretamente, com um entendimento completo do modelo de responsabilidade compartilhada e seus pontos cegos.

## Segurança de Containers na AWS

Um dos maiores problemas ao utilizar a AWS é proteger a rede de containers. Isto se deve à falta de contexto que o VPC tem para qualquer rede de sobreposição funcionando por cima. Os Grupos de Segurança da Amazon podem aplicar políticas de segurança a cada cluster, mas eles não conseguem fazer isso com os pods individuais, tornando esta tecnologia insuficiente. Quando seu negócio está tentando solucionar problemas ou obter melhor visibilidade das comunicações, o insight irá parar no tráfego entre os hosts no cluster, em vez dos pods, resultando em pontos cegos de segurança.

Como resultado, você precisa de duas soluções para controlar sua rede hospedada na nuvem. Uma trata de suas políticas de VM, enquanto a outra controla seus containers. Assim sendo, a criação de políticas de rede para uma única aplicação que inclua tanto containers quanto VMs requer o uso de soluções separadas. Seu negócio agora conta com dois conjuntos de controles a serem gerenciados, com toda a manutenção e administração que vem com eles. Isto acrescenta complexidade e risco, quando sua mudança para a nuvem foi provavelmente destinada a tornar sua infraestrutura e segurança mais fáceis, não mais complicadas.

## Falta de Visibilidade na AWS

62% dos tomadores de decisão de TI em grandes empresas acreditam que **sua segurança no local é mais forte do que a segurança na nuvem**. No local, esses especialistas em segurança sentem que têm controle sobre seu ambiente de TI e sobre os dados e comunicações dentro dele, e ao migrarem para a nuvem, eles perdem esse controle e visibilidade.

Com a microssegmentação inteligente, este não precisa ser o caso. Indo além dos sistemas de segurança AWS, o Guardicore Centra proporciona maior visibilidade, descobrindo automaticamente todas as aplicações e fluxos até o nível de processo (Camada 7). Ele inclui uma API da AWS que pode puxar dados de orquestração e tags para obter um contexto valioso para o mapeamento de aplicações, e permite que você faça uma baseline de sua infraestrutura de forma inteligente e informada, entendendo como suas aplicações se comportam e se comunicam, o que, por sua vez, permite detectar e alertar sobre mudanças. Como a solução Centra funciona em diversos fornecedores de nuvem, as empresas podem usá-la para ganhar visibilidade e aplicar controles de políticas em um ambiente heterogêneo sem estar vinculadas a nenhum fornecedor ou infraestrutura de nuvem.

## Criação e Controle de Políticas Application-Aware

No local, as empresas estão acostumadas a poder utilizar NGFWs (Next-Gen Firewalls) para proteger e segmentar aplicações. Na nuvem, a AWS não oferece a mesma funcionalidade. As aplicações de segmentação podem ser feitas utilizando grupos de segurança da AWS de forma restrita, suportando apenas o controle de tráfego até a Camada 4, portas e IPs. Com o Centra, você pode se beneficiar de políticas de segurança application-aware, que funcionam com aplicações AWS dinâmicas até o nível de processo. Ao invés de gerenciar dois ou mais conjuntos de controles, o Centra funciona em qualquer tipo de infraestrutura, incluindo data centers híbridos e multi-nuvem ou múltiplos fornecedores de IaaS, servidores físicos nas instalações, containers e microsserviços. Como a política segue a carga de trabalho, as empresas podem desfrutar de flexibilidade dinâmica sem comprometer a segurança.

Uma solução em todos esses ambientes promove uma atmosfera de simplicidade em seus data centers, com etiquetagem e agrupamento inteligentes que proporcionam uma visão de "um único painel de vidro" na mais complexa das infraestruturas. Sua equipe tem fácil navegação e visão dos problemas quando eles ocorrem, e conseguem definir a política de segmentação em questão de minutos, em vez de depender de tentativas e erros.

## Navegando nos Pontos Cegos para se Beneficiar com Segurança da AWS

Usar a AWS com segurança significa entender que é seu papel como cliente manter-se a par da segurança dos dados do cliente, bem como da plataforma, aplicação, gerenciamento de identidade e acesso, e qualquer configuração de sistema operacional, rede ou firewall. Usuários de nuvem precisam estar preparados para se esforçarem para garantir que suas cargas de trabalho sejam seguras, especialmente quando trabalham em ambientes multi-nuvem ou híbridos.

Quando implementada corretamente, a microssegmentação oferece uma maneira simples de proteger um ambiente híbrido, incluindo solucionar os desafios exclusivos dos containers na AWS e fornecer a capacidade de criar políticas dinâmicas de aplicação até o nível de processo. Acreditamos que as melhores soluções começam com a visibilidade fundamental, descobrindo automaticamente todos os fluxos e dependências da rede. Isso permite que sua empresa aproveite os últimos avanços tecnológicos sem aumentar o risco ou a complexidade para suas equipes de segurança.

**Sobre a Guardicore**

A Guardicore é a empresa de segmentação com soluções disruptivas para substituir o legado de firewalls tradicionais. Nossa abordagem, baseada unicamente em software, é independente da rede física, representando uma alternativa mais rápida ao firewall. Feita para empresas ágeis, a plataforma Guardicore oferece mais visibilidade e segurança na nuvem, datacenter e endpoints. Para mais informações acesse www.guardicore.com, nosso Twitter ou LinkedIn.



Guardicore