RESUMO DA SOLUÇÃO DA AKAMAI

Segmentação para ambientes de nuvem híbrida

Contenha ataques com segmentação para sua infraestrutura em nuvem

Com a crescente mudança de aplicações e cargas de trabalho para a nuvem, as equipes de segurança e nuvem enfrentam um número cada vez maior de desafios. Um deles é estender a segmentação e os princípios do Zero Trust para aplicações e cargas de trabalho em ambientes de nuvem. Com a Akamai Guardicore Segmentation, as organizações podem reduzir a superfície de ataque e conter ataques a aplicações e cargas de trabalho em seus ambientes de nuvem pública sem instalar agentes. Isso é obtido por meio da descoberta automática de aplicações, visualização abrangente de fluxos de nuvem, políticas de segmentação precisas e alertas de segurança de rede, tudo a partir de um único painel.

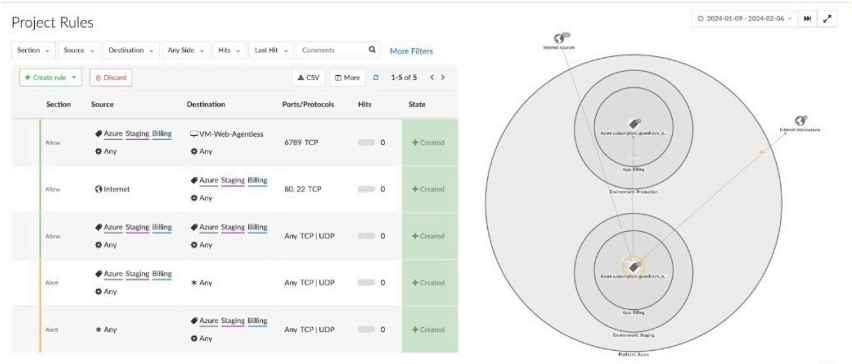
Desafios de nuvem específicos

As organizações modernas dependem cada vez mais da nuvem para gerenciar seus sistemas críticos e armazenar seus dados mais valiosos.

De acordo com o relatório Cost of a Data Breach de 2023 da IBM (em inglês), 82% das violações envolveram dados armazenados na nuvem — públicos, privados ou ambos. Os invasores geralmente conseguiam obter acesso a mais de uma plataforma de nuvem, com 39% das violações abrangendo vários ambientes e gerando um custo de US$ 4,75 milhões, o que é mais alto do que a média.

A natureza exclusiva e dinâmica da nuvem significa que as cargas de trabalho na nuvem estão mais expostas a ameaças externas do que os recursos locais. As equipes de segurança estão lidando com vários desafios específicos:

- **Baixa visibilidade**: a visibilidade do provedor de nuvem é baseada em registros brutos dos fluxos entre diferentes cargas de trabalho. Sem uma compreensão clara das relações entre diferentes cargas de trabalho e aplicações dentro de ambientes de nuvem, a criação de políticas de segurança eficazes se torna quase impossível.
- **Nenhuma política única**: criar uma política consistente em ambientes de nuvem híbrida usando apenas ferramentas nativas de segurança na nuvem é algo extremamente complexo. Isso ocorre porque cada instância de nuvem tem seus próprios objetos e regras e, portanto, suas próprias políticas, resultando em uma política fragmentada.
- **Falta de governança unificada:** a segurança nem sempre é uma prioridade na nuvem. Isso cria atrito entre as equipes de segurança e os proprietários de aplicações, que ativam cargas de trabalho sem levar em consideração a segurança.



Proteja uma aplicação do Azure usando sugestões de política automatizadas

Benefícios para o seu negócio

Visualize fluxos de nuvem usando uma única interface
Obtenha um profundo conhecimento de como suas cargas de trabalho e aplicações de nuvem interagem usando um mapa dinâmico de dependências de rede e aplique controles de segurança facilmente.

Aplique uma política de segmentação consistente
Implemente uma única solução de segmentação que funcione consistentemente em ambientes de nuvem híbrida, evitando soluções específicas de fornecedores que criam silos de segurança.

Impeça violações
Adapte as políticas de segurança a qualquer mudança em seu ambiente de nuvem, livrando sua equipe de atualizações manuais.

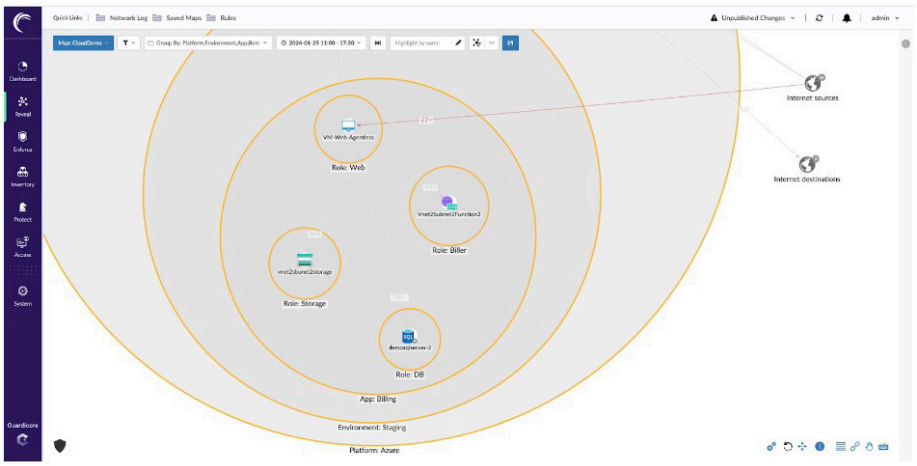
Akamai

Evite ameaças à segurança na nuvem

A Akamai Guardicore Segmentation estende sua segmentação líder do setor para aplicações e cargas de trabalho em nuvem. Ao estender a segmentação para seus ativos na nuvem, qualquer conexão não autorizada é automaticamente interrompida, restringindo, assim, a movimentação lateral e os danos causados por violações ou incidentes de ransomware.

Principais recursos

- **A visibilidade e a aplicação abrangentes sem agente nativas da nuvem** permitem que os administradores visualizem cargas de trabalho na nuvem usando um mapa interativo quase em tempo real de fluxos de rede reais, conhecendo as dependências das aplicações e reunindo equipes de DevOps e SecOps na governança de segurança da rede na nuvem.
- **O mecanismo híbrido que aproveita vários pontos de aplicação** permite que uma organização defina de maneira simples a intenção da política de rede e que deixe a política da Akamai Guardicore Segmentation cuidando do resto, decidindo dinamicamente quais pontos de aplicação com ou sem agente são usados em todo o data center.
- **Os recursos integrados de firewall de análise de reputação e inteligência de ameaças** foram projetados para reduzir o tempo de detecção e de resposta a incidentes em caso de violação.
- **A solução escalável e segura** garante que os dados não deixem seu ambiente de nuvem e a arquitetura da solução seja dimensionada automaticamente dentro dele.



Um mapa único para ambientes locais e de nuvem híbrida

Acesse akamai.com/guardicore para obter mais informações.

 | Suporte | | Publicado em 02/24