RESUMO DA SOLUÇÃO DA AKAMAI

Como proteger cargas de trabalho na AWS com a Akamai Guardicore Segmentation

As empresas continuam utilizando recursos PaaS na Amazon Web Services (AWS), e muitas estão migrando suas cargas de trabalho críticas para a nuvem pública. Essas empresas estão percebendo benefícios como redução de custos, escalabilidade e desempenho aprimorados e maior agilidade nos negócios. No entanto, essa migração para a nuvem traz preocupações de segurança urgentes, como:

Novo conjunto de ferramentas

Operar em um ambiente de nuvem exige um conjunto completamente novo de controles de segurança. Esses controles precisam oferecer suporte à AWS tanto na nuvem quanto via AWS Outposts no local, além de cargas de trabalho em nuvens híbridas. Grupos de segurança na nuvem existentes podem ser suficientes para ativos e recursos na Nuvem AWS, mas esses controles não protegem ativos ou recursos relacionados em outros ambientes. Isso significa que sua equipe precisa gerenciar várias ferramentas de segurança, o que pode resultar em possíveis lacunas de segurança.

Novo modelo de operação de segurança

Como parte do Modelo de responsabilidade compartilhada da AWS, ao utilizar recursos da AWS na nuvem ou no local, a responsabilidade da Amazon se limita à proteção da infraestrutura que executa todos os serviços oferecidos na Nuvem AWS. No entanto, qualquer aplicativo ou software utilitário instalado nessas instâncias, bem como a configuração dos grupos de segurança, são de responsabilidade exclusiva do usuário. Isso inclui também a proteção e monitoramento do tráfego, tanto norte-sul quanto leste-oeste, além da implantação de controles para detectar, prevenir e responder a violações.

Visibilidade e controle reduzidos da infraestrutura

As mesmas vantagens que tornam o ambiente AWS operacionalmente atraente também podem resultar em menor controle e visibilidade dos ativos que estão espalhados por várias contas, nuvens privadas virtuais (VPCs) e grupos de segurança de rede na AWS, assim como de todo o ecossistema híbrido de uma organização.

Principais benefícios

- Solução completa para proteger cargas de trabalho na AWS, incluindo recursos PaaS, permitindo que as equipes de DevOps e segurança concentrem recursos escassos em tarefas críticas, e não no gerenciamento da segurança do data center
- Gerenciar e impor políticas rigorosas de microssegmentação que se estendem além da AWS, incluindo ativos no local e até mesmo em nuvens públicas
- Detectar de forma confiável violações de políticas e responder a elas em tempo real
- Proteger ambientes contra possíveis violações utilizando múltiplos métodos de detecção e prevenção de intrusões, incluindo análise de reputação e tecnologia deception dinâmica em tempo real

Akamai Guardicore Segmentation para segurança na AWS

A Akamai Guardicore Segmentation é uma solução unificada para visibilidade e aplicação de políticas para cargas de trabalho e recursos PaaS em execução em suas nuvens, Outposts e ambientes híbridos da AWS. Ela fornece microssegmentação e visibilidade no nível dos aplicativos, além de recursos de detecção e resposta a violações.

Descoberta e visibilidade automáticas

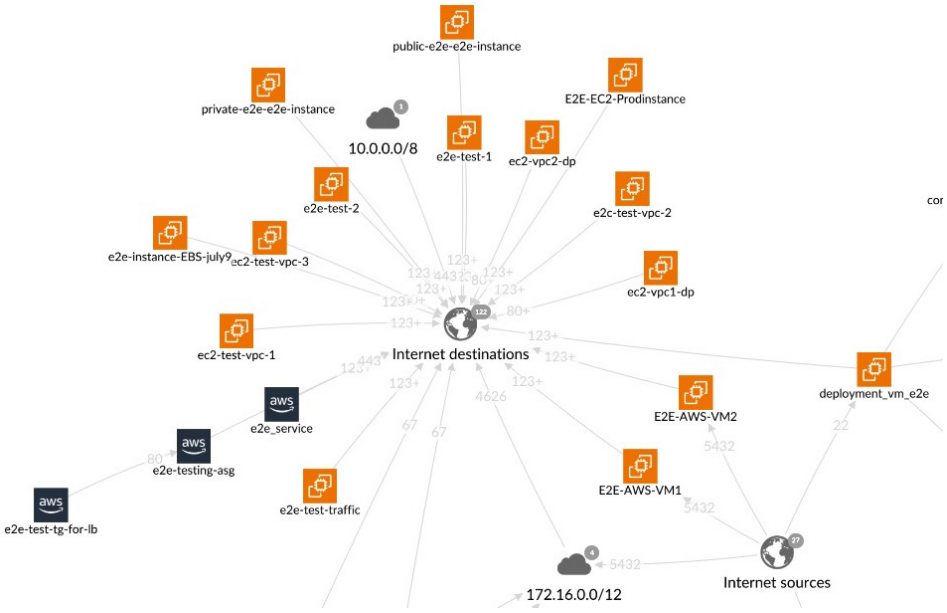
- Visualize aplicativos, recursos e seus fluxos de comunicação automaticamente
- Entenda o comportamento dos aplicativos e defina sua linha de base rapidamente
- Mapeie dependências de aplicativos com visibilidade granular até o nível do processo (Camada 7)

Segmentação e aplicação de políticas eficazes

- Defina políticas de segmentação em questão de minutos
- Obtenha recomendações automáticas de políticas
- Use funções inteligentes de identificação e agrupamento que simplificam a navegação entre ambientes complexos

Detecção de ameaças e resposta a incidentes

- Obtenha valor desde o primeiro dia, sem necessidade de configuração
- Obtenha diversos métodos de detecção que abrangem todos os tipos de ameaça
- Aproveite a tecnologia deception, com cobertura de rede completa



Visualize e proteja aplicativos e recursos na AWS com a Akamai Guardicore Segmentation

> Ao escolher a Akamai Guardicore Segmentation, conseguimos preencher lacunas de segurança críticas relacionadas à microssegmentação e à visibilidade no nível dos aplicativos, bem como à detecção e resposta a violações, abrangendo servidores AWS e no local.
>
> — **Líder de equipe de DevOps**
> Empresa de biotecnologia

Proteja de forma contínua suas cargas de trabalho e recursos PaaS na AWS. Saiba mais em akamai.com/guardicore.