GUIA DE COMPARAÇÃO

Akamai Guardicore Segmentation versus soluções tradicionais de microssegmentação

Visibilidade incomparável

Para entender o que está acontecendo no seu ambiente, é essencial ter visibilidade das comunicações entre as cargas de trabalho. A visibilidade verdadeiramente eficaz significa ser capaz de saber, a qualquer momento, o que cada carga de trabalho está fazendo com todo o contexto. Além disso, os recursos de agrupamento e filtragem para ativos e regras são componentes essenciais para a criação de políticas de forma rápida e eficaz.

Akamai	Microssegmentação tradicional
Visualize facilmente todo o ambiente O agente Akamai Guardicore Segmentation é um firewall baseado em host executado em sistemas operacionais modernos e legados, fornecendo visibilidade total dos fluxos de rede até os processos individuais e níveis de serviço para sistemas operacionais Windows e Linux, juntamente com cobertura para pontos de extremidade MacOS.	**Visibilidade parcial para itens legados** Não há visibilidade em sistemas Microsoft Windows anteriores ao Windows 2002. Isso ocorre porque o agente das soluções tradicionais de microssegmentação depende de um firewall do Windows, que só estava disponível em sistemas posteriores a 2002. Para sistemas Linux, seus agentes suportam apenas a visibilidade L4.
Contexto rico e incomparável Quando se trata de visibilidade, ter contexto e detalhes adequados é fundamental. Nossa solução coleta, além de dados de fluxo, contexto crítico, como informações de processo, arquivo, nível de patch e muito mais.	**Contexto mínimo** Coleta apenas de informações sobre fluxos e máquinas, sem detalhes contextuais essenciais, como processo e arquivo. Isso torna o processo de compreensão das dependências do aplicativo mais trabalhoso e demorado.
Sem limitação no tipo ou número de rótulos Não temos restrições quanto ao tipo ou número de rótulos que você pode ter, permitindo flexibilidade e suportando casos de uso adicionais. Isso poupará o esforço de ter que converter seus rótulos existentes de bancos de dados de gerenciamento de configuração (CMDBs) e outras fontes de dados.	**Rotulagem rígida** Com uma hierarquia de rotulagem fixa e predefinida, as soluções tradicionais forçam você a rotular suas aplicações usando uma quantidade definida determinada apenas por elas, independentemente dos requisitos do seu próprio ambiente e das necessidades de negócios.
Rotulagem orientada por IA A detecção e a rotulagem de aplicações usando inteligência artificial ajudarão você a identificar aplicações quando não houver CMDB confiável e atribuir automaticamente o rótulo correto.	**Sem CMDB? Você está em um beco sem saída...** Com a rotulagem manual e uma hierarquia de quatro rótulos pré-configurada, se a sua organização não tiver um CMDB no qual confiar, o processo de rotulagem se tornará extremamente complicado.

Akamai

Cobertura líder do setor

Um dos principais elementos de uma boa solução de microssegmentação é a capacidade de proteger ativos críticos, independentemente de onde eles sejam implantados ou acessados - legados ou modernos, Windows ou Linux, no local ou virtualizados, contêineres e muito mais.

Akamai

Compatibilidade completa com Windows e Linux

Os agentes da Akamai Guardicore Segmentation são compatíveis com todos os sistemas operacionais Windows e Linux, novos e legados, pois nossa solução não depende da infraestrutura subjacente.

Compatibilidade abrangente com contêineres

Visibilidade completa para ambientes em contêineres enquanto aproveita os controles da Container Network Interface (CNI) para aplicação.

Microssegmentação tradicional

Compatibilidade limitada com Windows e Linux

A aplicação de políticas depende do firewall do Windows para ambientes Windows e iptables para ambientes Linux. Isso inevitavelmente significa proteção limitada ou inexistente para alguns sistemas operacionais Windows legados e nenhuma regra de nível de processo L7 para ambientes Linux.

Compatibilidade limitada com contêineres

A aplicação depende de iptables e cálculos de políticas constantes, que não são dimensionados em um ambiente de contêiner e causam latência e tempo de inatividade.

Crie políticas simples. Sem demora.

Um bom mecanismo de políticas permite expressar sua intenção usando o menor número possível de regras, sem forçar restrições de linguagem de políticas. Isso também ajudará a minimizar o trabalho de gerenciamento de políticas, fornecendo automação e assistentes.

Akamai

Permitir e negar

Oferecemos compatibilidade com regras de lista de permissões e de listas de bloqueio, e qualquer combinação entre elas. Isso permite que as equipes de segurança e de resposta a incidentes respondam rapidamente em qualquer cenário de segurança, eliminando a necessidade de primeiro colocar na lista de permissões todos os fluxos legítimos.

Modelos de política para uma variedade de casos de uso

Modelos prontos para uso e fluxos de trabalho de criação de políticas para cenários comuns — mitigação de ransomware, proteção de aplicativos, segmentação de ambiente e muito mais. Os modelos ajudam a economizar tempo e reduzir erros humanos.

Critérios ricos para políticas

Os critérios para políticas podem incluir origem, destino, porta, protocolo, processo, serviço (por exemplo, Agendador de tarefas comumente usado por ransomware), usuário e nome de domínio totalmente qualificado (FQDN).

Microssegmentação tradicional

Lista de permissões com compatibilidade limitada com regras de negação

A adesão ao modelo de listas de permissões, que, apesar de seguro, é muito demorado, não permite que as soluções tradicionais de segmentação respondam automaticamente a ameaças conhecidas, que exigem bloqueio rápido.

Um conjunto limitado de modelos

Os modelos de segmentação são compatíveis principalmente com ambientes Microsoft. Não há compatibilidade com modelos para casos de uso de segmentação comuns, como delimitação de acesso (ringfencing) e mitigação e limpeza de ransomware.

Critérios limitados

Sem política no nível de processos L7 para sistemas operacionais Linux nem capacidade de criar políticas com base em serviços individuais do Microsoft Windows.

Segurança em primeiro lugar

O combate a ameaças de segurança complexas, como o ransomware, requer uma abordagem abrangente com relação à segurança. Embora a segmentação seja prescrita pelo Instituto Nacional de Padrões e Tecnologia (NIST) e pela Casa Branca como uma resposta fundamental, é necessária uma abordagem integrada à segurança e à detecção de violações para manter sua organização segura.

Akamai	Microssegmentação tradicional
Prevenção e mitigação de ransomware A Akamai Guardicore Segmentation fornece modelos prontos para uso para todas as fases da cadeia de eliminação de ataques, desde a prevenção até a contenção e mitigação.	**Nenhum modelo de ransomware** As soluções tradicionais são limitadas quanto à sua capacidade de bloquear ataques de ransomware com modelos prontos para uso.
Analisar os pontos de extremidade para detectar ameaças e verificar conformidade Nossa ferramenta Insight, com base em Osquery, permite que você consulte servidores e pontos de extremidade em tempo real para detectar ameaças de malware e verificar conformidade.	**Sem detecção em tempo real** As soluções tradicionais não conseguem detectar atividades maliciosas em tempo real no data center.
Recursos com tecnologia "deception” Com base em uma tecnologia patenteada, o agente Akamai Guardicore Segmentation redireciona sessões bloqueadas e com falha para um mecanismo dinâmico de engano para análise e quarentena.	**Sem capacidade de quarentena** As soluções tradicionais carecem de recursos de engano, bem como da capacidade de detectar ou colocar em quarentena máquinas usando indicadores de comprometimento conhecidos (IOCs).
Serviço de busca de ameaças gerenciado A Akamai oferece serviços gerenciados de busca de ameaças que ampliam os recursos da sua equipe de segurança e permitem que sua organização se antecipe às ameaças mais recentes.	**Sem serviços de busca de ameaças** Os fornecedores tradicionais não podem oferecer serviços de busca de ameaças desenvolvidos com base em sua solução, o que pode ser um diferencial crítico diante do aumento de ransomware e malware.
Firewall de inteligência para ameaças Para evitar comportamentos maliciosos conhecidos, a Akamai Guardicore Segmentation bloqueia IPs, arquivos e hashes maliciosos usando regras automáticas de firewall.	**Sem feeds de ameaças** Sem um recurso semelhante, as soluções tradicionais não conseguem impedir o acesso de IPs e URLs maliciosos conhecidos.

Operações ou desempenho e latência

A baixa latência é fundamental para um projeto de segmentação que funcione. Isso significa que você deve ser capaz de expandir sua política com mais regras, rótulos por ativos e outros objetos de política, tudo sem adicionar latência.

Akamai

Mecanismo otimizado para latência

Nosso mecanismo de segmentação foi desenvolvido para cenários de grande escala. Para chegar nesse resultado, é usado um mecanismo de filtragem otimizado, resultando em um tempo de latência relativamente insensível ao tamanho da política.

Microssegmentação tradicional

Mais regras aumentam a latência

Os agentes trazem mais latência à medida que a quantidade e o tamanho das regras aumentam. Os iptables do Linux simplesmente não foram desenvolvidos para se dimensionar ao nível do tráfego leste-oeste de porte empresarial. O resultado é uma latência significativa que aumenta diretamente com o tamanho da política.

Para obter mais informações sobre o Akamai Guardicore Segmentation ou para solicitar uma demonstração personalizada do produto, acesse akamai.com/guardicore.

©2023 Akamai Technologies | Suporte | | Publicado em 07/23