RESUMO DO PRODUTO DA AKAMAI

Akamai Guardicore Segmentation

Impeça a movimentação lateral com visibilidade granular e controles de microssegmentação

A infraestrutura de TI corporativa continua evoluindo de data centers tradicionais no local para arquiteturas de nuvem e nuvem híbrida, com uma combinação de plataformas e modelos de implantação de aplicações. Embora essa transformação digital esteja ajudando muitas organizações a alcançar maior agilidade nos negócios, reduzir os custos de infraestrutura e permitir o trabalho remoto, ela também está criando uma superfície de ataque maior e mais complexa que não tem um perímetro bem definido. Cada servidor individual, máquina virtual, instância de nuvem e ponto de extremidade agora é um possível ponto de exposição. E com a prevalência de ameaças como ransomware e vulnerabilidades de dia zero, os invasores estão se tornando mais adeptos da movimentação lateral visando alvos de alto valor quando encontram uma brecha.

A Akamai Guardicore Segmentation oferece a maneira mais simples, rápida e intuitiva de aplicar os princípios Zero Trust em sua rede. Ela foi projetada para impedir a movimentação lateral através da visualização da atividade em seus ambientes de TI, implementação de políticas precisas de microssegmentação e detecção rápida de possíveis violações.

Principais recursos da solução

Segmentação granular e impulsionada por IA

Implemente políticas com apenas alguns cliques usando recomendações de IA, modelos para remediação de ransomware e outros casos de uso comuns, além de atributos precisos de carga de trabalho, como processos, usuários e nomes de domínio

Visibilidade histórica e em tempo real

Mapeie dependências de aplicações e fluxos nos níveis de usuários e processos em tempo real ou historicamente

Amplo suporte a plataformas

Abranja sistemas operacionais modernos e legados em servidores bare metal, máquinas virtuais, contêineres, IoT e instâncias na nuvem

Rotulagem flexível de ativos

Adicione contexto avançado com uma hierarquia de rotulagem personalizável para visibilidade e execução, e integração com ferramentas de orquestração e bancos de dados de gerenciamento de configuração para rotulagem automatizada

Vários métodos de proteção

Integre recursos de inteligência contra ameaças, defesa e detecção de violações para reduzir o tempo de resposta a incidentes

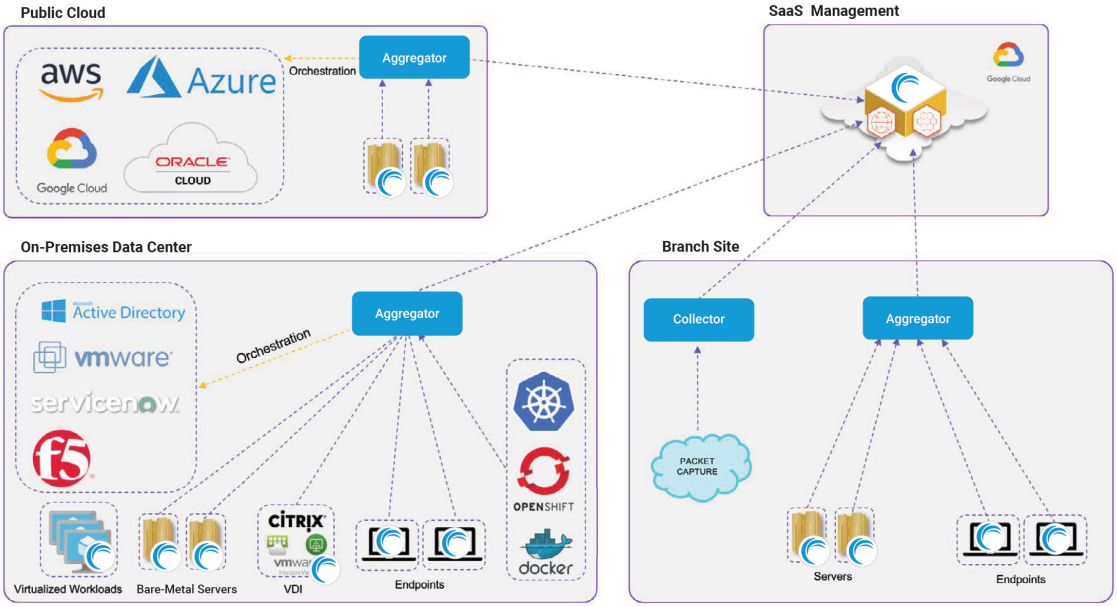
VANTAGENS PARA SUA EMPRESA

- Prevenção contra ransomware
- Obtenção da segurança Zero Trust
- Aceleração da conformidade
- Isolamento de aplicações essenciais
- Migrações seguras para a nuvem
- Proteção da força de trabalho remota
- Proteção de pontos de extremidade
- Avanço além de firewalls internos

Como funciona

A Akamai Guardicore Segmentation coleta informações detalhadas sobre a infraestrutura de TI de uma organização por meio de uma combinação de sensores baseados em agentes, coletores de dados baseados em rede, registros virtuais de fluxo de nuvem privada de provedores de nuvem e integrações que permitem a funcionalidade sem agentes. O contexto relevante é adicionado a essas informações por meio de um processo de rotulagem flexível e altamente automatizado que inclui integração com fontes de dados existentes, como sistemas de orquestração e bancos de dados de gerenciamento de configuração.

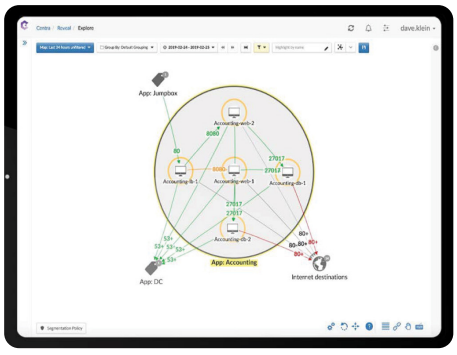
Topologia de infraestruturas



A maioria dos clientes utiliza o gerenciamento de SaaS, mas também estão disponíveis opções de gerenciamento no local.

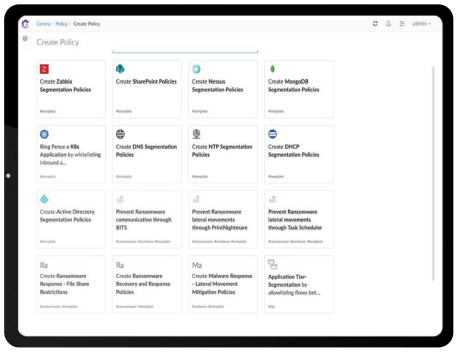
Mapa de redes

O resultado é um mapa dinâmico de toda a infraestrutura de TI que permite que as equipes de segurança visualizem a atividade com granularidade no nível de usuário e de processo, em tempo real ou por histórico. Esses insights detalhados, combinados com fluxos de trabalho de políticas com inteligência artificial, tornam a criação de políticas de segmentação rápida, intuitiva e baseada no contexto real da carga de trabalho.



Modelos

A criação de políticas é facilitada com modelos pré-criados para os casos de uso mais comuns. A imposição de políticas é completamente dissociada da infraestrutura subjacente, de modo que as políticas de segurança podem ser criadas ou alteradas sem modificações complexas na rede ou tempo de inatividade. Além disso, as políticas seguem a carga de trabalho, independentemente de onde ela reside, em data centers locais ou ambientes na nuvem pública. Nossos recursos de segmentação são complementados por um conjunto sofisticado de mecanismos de proteção contra ameaças e detecção de violações, assim como pelo Akamai Hunt, nosso serviço gerenciado de identificação de ameaças.



Proteção abrangente em escala

Todos os ambientes

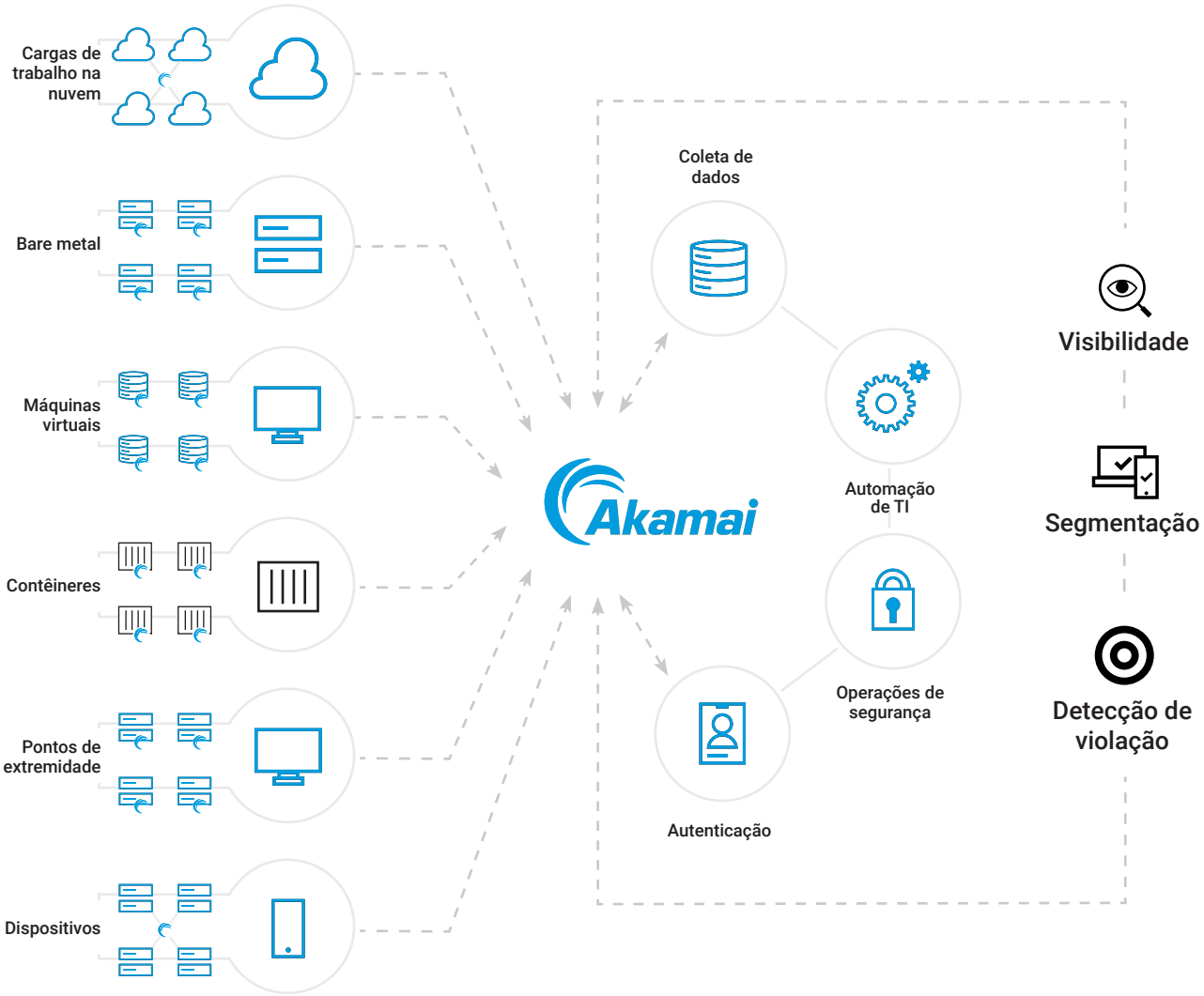
Proteja cargas de trabalho em ambientes de TI complexos com uma combinação de cargas de trabalho locais, máquinas virtuais, sistemas legados, contêineres e orquestração, instâncias de nuvem pública/privada e IoT/OT

Segurança simplificada

Simplifique o gerenciamento de segurança com uma plataforma que fornece visualização de rede, segmentação, defesa contra ameaças, recursos de detecção de violações e aplicação orientada de políticas para iniciativas Zero Trust

Desempenho e escalabilidade empresariais

Comece por uma proteção focada dos seus ativos digitais mais críticos e amplie para proteger toda a sua empresa sem complexidade, mudanças de infraestrutura ou gargalos de desempenho



Plataformas e tecnologias compatíveis

- A Akamai Guardicore Segmentation foi projetada para se integrar à sua infraestrutura existente.
- Nosso suporte a sistemas operacionais se expande continuamente de acordo com as necessidades dos nossos clientes.
- Confira nossa página de parceiros de tecnologia para obter uma lista completa das nossas integrações.

Sistemas operacionais

Linux

Apple

Microsoft

Unix

Provedores de nuvem pública

Hipervisores

Orquestração de hipervisão

Gateways de segurança

Orquestração e mecanismos de contêineres

Navegadores para console da Web

Requisitos mínimos de memória e sistema

Management Server
32 GB RAM, 8 vCPUs, 530 GB

Aggregator
4 GB RAM, 4 vCPUs, 30 GB

Deception Server
32 GB RAM, 8 vCPUs, 100 GB

ESC Collector
2 GB RAM, 2 vCPUs, 30 GB

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

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

 | Suporte | | Publicado em 03/25