RESUMO DA SOLUÇÃO DA AKAMAI

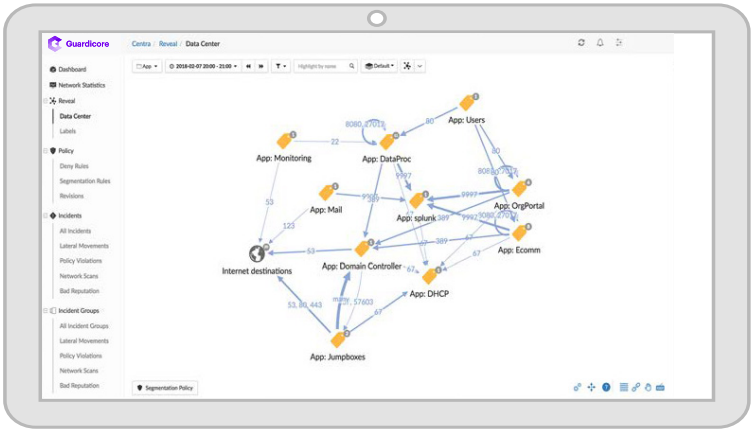
Microssegmentação rápida em ambientes híbridos com a Akamai Guardicore Segmentation

O caminho para implementar a microssegmentação não é uma linha reta; há muitas reviravoltas quando você começa a descobrir, entender e controlar os fluxos de aplicações no seu ambiente de TI. Mas sem a abordagem certa para navegar pelo caminho, você pode encontrar vários desafios. Os pontos cegos da rede geralmente impedem a descoberta suficiente e o mapeamento de comunicação de aplicações, cargas de trabalho e processos subjacentes. Mecanismos rígidos de política podem forçar decisões abrangentes, que correm o risco de interromper as aplicações. A expressão de política inconsistente nos sistemas operacionais pode resultar em brechas de segurança perigosas. Por fim, integrações complexas, e frequentemente manuais, de dados de violação de política com ferramentas de detecção de violação podem retardar a investigação e a resposta a incidentes. A Akamai Guardicore Segmentation ajuda você a ter sucesso na implementação da microssegmentação em três etapas.

Etapa 1: Revelar

Detecte aplicações automaticamente e visualize fluxos

A Akamai Guardicore Segmentation apresenta a melhor visibilidade da categoria, que descobre e visualiza automaticamente todas as aplicações, cargas de trabalho e fluxos de comunicação com contexto no nível do processo, independentemente de onde residam. Você terá a mesma visualização para ativos locais, na nuvem, em várias nuvens e muito mais. Essa visualização, juntamente com a importação automática de metadados de orquestração, permite que suas equipes de segurança rotulem e agrupem de forma rápida e fácil todos os ativos e aplicações, agilizando o desenvolvimento de políticas.



Proteja aplicações essenciais onde quer que elas residam

Independente de plataforma

A Akamai Guardicore Segmentation pode visualizar os ativos e aplicar a política de segurança entre infraestruturas: no local, na nuvem e em várias nuvens

Agilidade na implantação da política

Sugestões automatizadas de regras, um mecanismo de políticas flexível e uma interface de usuário intuitiva tornam a criação e a aplicação de políticas menos demoradas

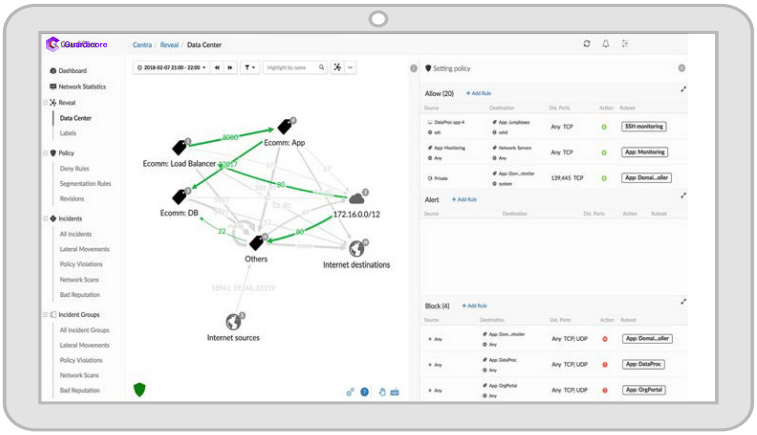
Integração de detecção e resposta a violações

Visualize violações de políticas e responda rapidamente a ameaças ativas, protegendo seus ativos mais essenciais, independentemente de onde eles residam

Etapa 2: Criar

Projete, teste e implante políticas rapidamente

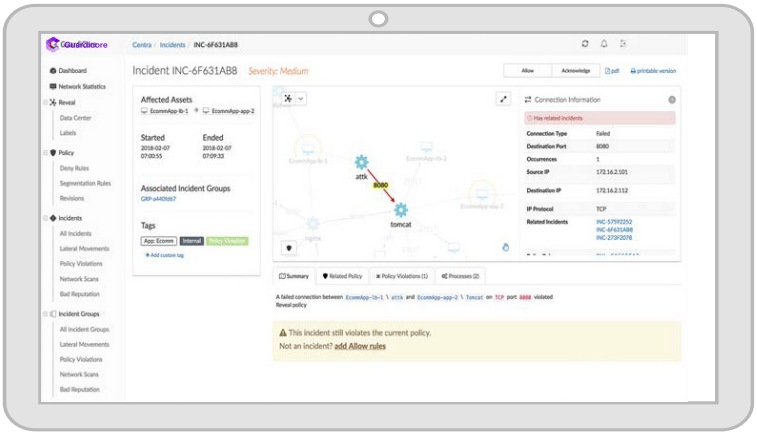
A Akamai Guardicore Segmentation simplifica o desenvolvimento e o gerenciamento de políticas de microssegmentação. Um único clique em um fluxo de comunicação no mapa Revelar gera sugestões de regras automatizadas com base em observações históricas, permitindo que você crie rapidamente uma política sólida. Um fluxo de trabalho intuitivo e um mecanismo de política flexível suportam o refinamento contínuo de políticas e reduzem erros dispendiosos.



Etapa 3: Aplicar

Forneça segurança sólida em qualquer ambiente

Com a capacidade de impor a política de comunicação no nível da rede e do processo em todos os sistemas, a Akamai Guardicore Segmentation mantém a segurança, independentemente das limitações de execução do sistema operacional. Além disso, os recursos integrados de detecção e resposta a violações permitem que você veja as violações de política no contexto de uma violação ativa, permitindo identificar rapidamente o método de ataque e corrigi-lo.



Acesse akamai.com/guardicore para obter mais informações.

 | Suporte | | Publicado em 06/23