RESUMO DA SOLUÇÃO DA AKAMAI

Gerenciamento do acesso à identidade do usuário com segmentação

Uma camada adicional de controle fundamental para data centers híbridos modernos

Reduzir a superfície de ataque para os ambientes de TI de hoje é mais do que apenas criar controles rígidos em torno de aplicações específicas, protegendo-as de danos. Essa é uma excelente primeira etapa e certamente pode ajudar em alguns casos de uso, como contenção de violação ou conformidade. No entanto, sem uma solução de segmentação que ofereça suporte ao gerenciamento do acesso à identidade do usuário, sua organização terá um ponto cego de segurança que inclui todas as pessoas que usam ou entram em sua rede.

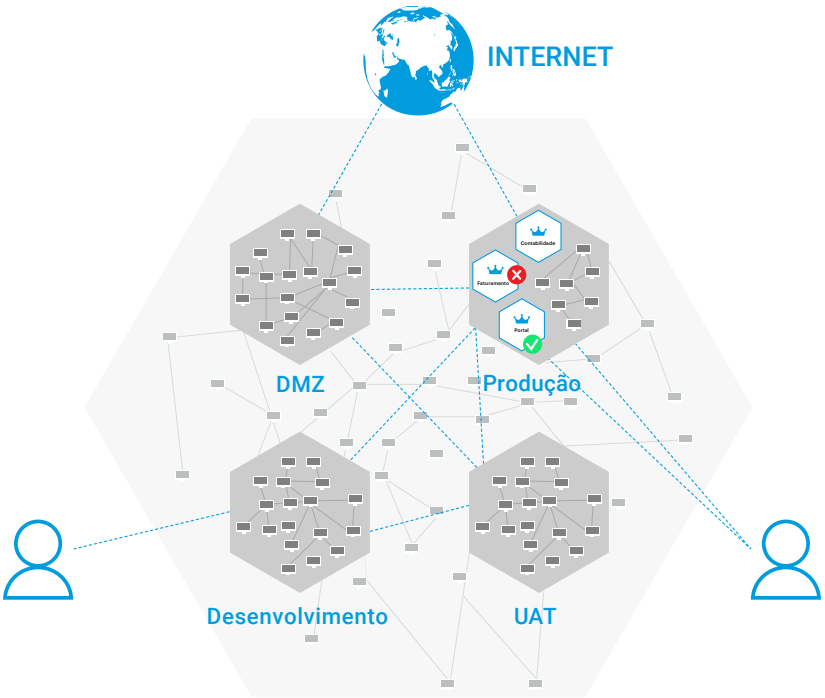
Depois que a segmentação de aplicações estiver em vigor, a próxima etapa essencial será aproveitar sua solução de segmentação para criar políticas sobre quem pode acessar essas aplicações, garantindo que elas sejam seguras em toda e qualquer arquitetura em sua rede.

Casos de uso: segmentação para acesso à identidade do usuário

Gerenciar o acesso do usuário

Usando um grupo de usuários do Active Directory, a Akamai Guardicore Segmentation pode controlar o acesso do usuário a qualquer aplicação ou carga de trabalho, a partir de qualquer ambiente. Grupos de usuários específicos têm acesso a servidores específicos, por meio de portas ou processos específicos, enquanto outros não têm. Os grupos de usuários têm suas próprias permissões, enquanto todos os outros acessos podem ser bloqueados. Sem a necessidade de um firewall centralizado, você pode usar o controle de acesso granular entre cargas de trabalho em segmentos específicos da rede.

Controle de acesso do usuário



Por que usar a segmentação para o controle de acesso do usuário?

Controle o acesso do usuário em qualquer lugar
As políticas funcionam em notebooks, desktops, VDI, servidores virtuais ou bare-metal e infraestrutura em nuvem

Segmentação definida por software
Sem alterações de rede ou arquitetura, sem cabos, sem tempo de inatividade do servidor e sem reinicialização de sistemas

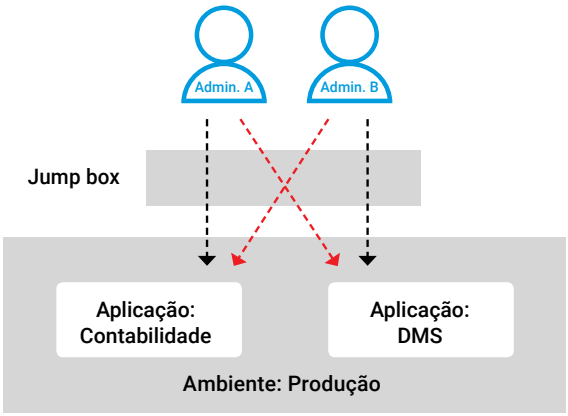
Rápida e potente
As políticas são simples e intuitivas de criar e entram em vigor imediatamente em sessões novas e ativas

Econômica
Em comparação com casos de uso semelhantes atendidos com a infraestrutura tradicional de jump box, os custos demonstraram ser até 60% menores

Akamai

Lidar com acesso simultâneo do usuário

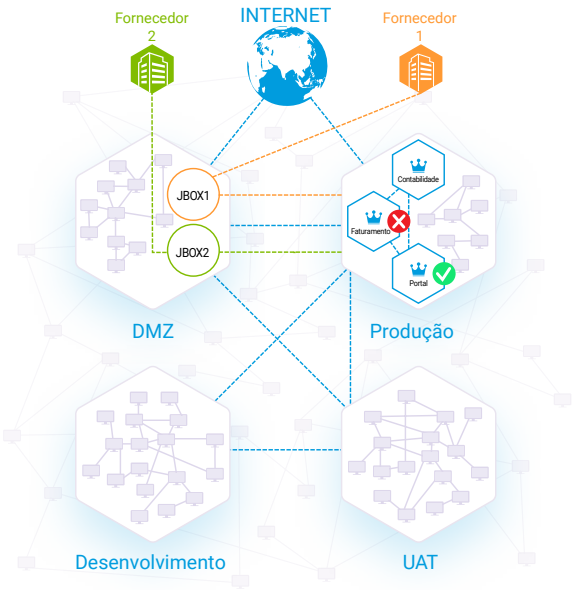
Os administradores podem acessar diferentes aplicações por meio da mesma jump box ou servidor de terminal, mesmo quando estiverem conectados ao mesmo tempo. Enquanto isso, políticas diferentes funcionarão de modo uniforme, permitindo que um usuário acesse o que tem direito, enquanto o outro permanecerá bloqueado, sem interrupção do serviço ou acesso do próprio usuário.



Controlar o acesso de terceiros

Com base na identidade do usuário, a Akamai Guardicore Segmentation pode controlar o gerenciamento do acesso de terceiros, por exemplo, de fornecedores externos ou provedores de SaaS. Com a ajuda de grupos de usuários, cada conexão de terceiros pode ter suas próprias políticas de acesso definidas para o data center e para aplicações específicas, concedendo permissões para o que o usuário precisa para sua própria função e nada mais.

Controle de acesso de terceiros



Juntos, a segmentação de aplicações e o gerenciamento do acesso à identidade do usuário são o golpe duplo mais forte para proteger o data center corporativo moderno.

Quer saber mais sobre como eles funcionam em conjunto? Entre em contato para falar com um dos nossos especialistas.