RESUMO DO PRODUTO DA AKAMAI

Akamai Guardicore Access

ZTNA e microssegmentação unificados

Um único console para visibilidade e controle simplifica e acelera o Zero Trust

As organizações estão adotando rapidamente a segurança Zero Trust para deter o ransomware, cumprir normas de conformidade e proteger sua força de trabalho híbrida e infraestrutura de nuvem. O Zero Trust Network Access (ZTNA) e a microssegmentação são as duas soluções mais críticas para empresas que estão migrando para uma arquitetura Zero Trust. Juntos, eles ajudam a reduzir a superfície de ataque, contêm violações e fornecem melhor controle de acesso com uma experiência de usuário aprimorada.

O poder da unificação

O Akamai Guardicore Access combina segmentação e ZTNA; eles são implantados com um único agente e gerenciados com um único console. Essa abordagem inovadora garante visibilidade abrangente do usuário até a carga de trabalho (norte-sul) e do ponto de extremidade até o ponto de extremidade ou a carga de trabalho (leste-oeste), permitindo o controle de acesso a aplicativos com base em identidade e a segmentação de pontos de extremidade de uma só vez. Ao combinar essas tecnologias, as empresas se beneficiam de uma estrutura de segurança robusta que fortalece as defesas de rede, mitiga os riscos e promove um ambiente seguro e em conformidade com as normas.

A Plataforma Akamai Guardicore é a primeira plataforma de segurança a combinar microssegmentação e ZTNA líderes do setor para ajudar as equipes de segurança a evitar ataques de ransomware, garantir a conformidade regulatória e proteger tanto a força de trabalho híbrida quanto a infraestrutura de nuvem.

Pela primeira vez, as organizações podem implementar a segmentação para minimizar a superfície de ataque, ao mesmo tempo que gerenciam facilmente o acesso de sua força de trabalho híbrida de todos os lugares, com um único agente e um único console em todos os tipos de ativos e infraestruturas.

Principais recursos

Visibilidade completa
Obtenha uma perspectiva total de sua rede com visibilidade completa no mapa e nos registros, além de insights sobre os padrões de acesso dos usuários finais. Isso só é possível combinando segmentação e ZTNA em um único produto. Veja trajetos de conexão, de pontos de extremidade a cargas de trabalho, até o nível do processo. A visibilidade quase em tempo real e histórica torna a análise forense mais fácil e a mitigação mais rápida.

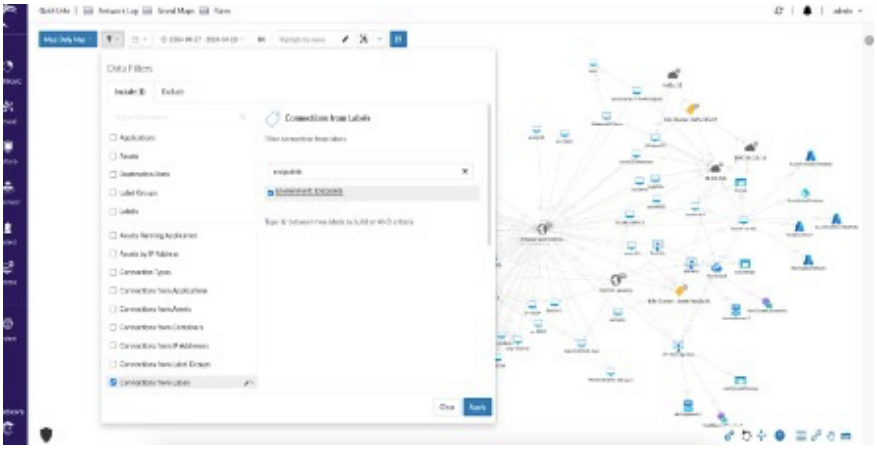
Benefícios para os seus negócios

Console único, agente único
Implemente a segmentação para minimizar a superfície de ataque ao mesmo tempo que gerencia facilmente o acesso de uma força de trabalho híbrida de todos os lugares — com um único agente e um único console

Ampla cobertura
Aplique controles de acesso em todos os lugares e proteja as forças de trabalho remotas e presenciais

Política unificada
Aplique políticas de tráfego leste-oeste e acesso norte-sul sem ter que alterar a sintaxe ou os consoles, obtendo a forma mais simples e eficaz de tomar decisões com base na segurança Zero Trust.

Descoberta de aplicativos
Acelere o tempo de aplicação de políticas identificando rapidamente os aplicativos que precisam de permissões de acesso. Descubra facilmente seus aplicativos privados e obtenha informações valiosas sobre seus padrões de uso, incluindo acesso e frequência do usuário.



Descubra facilmente os aplicativos para os quais o acesso é necessário

Sincronização de políticas de acesso e segmentação
Sincronize automaticamente controles de acesso e regras de segmentação para reduzir dependências entre equipes e eliminar a possibilidade de erros humanos.

Principais casos práticos

Proteção abrangente contra ransomware: reduza a probabilidade e o impacto de ataques de ransomware e outros malwares com políticas baseadas em identidade e máquina-a-máquina. Certifique-se de que os pontos de extremidade acessem os recursos com base no modelo de mínimo privilégio enquanto aplica controles granulares de acesso.

- Proteja ativos de alto valor: permita que os usuários acessem ativos críticos com base em controles de acesso seguros e bloqueie o tráfego direto de VPNs
- Restrinja usuários privilegiados: bloqueie o tráfego de VPNs para portas administrativas exploráveis para garantir acesso seguro aos administradores

Distribuição da força de trabalho: ofereça suporte a modelos de trabalho em todos os lugares com a aplicação de controles de acesso rigorosos, garantindo que cada dispositivo se conecte apenas aos recursos de que precisa. Isso minimiza a superfície de ataque e reduz o movimento lateral dentro da rede.

Conformidade: implemente políticas de segmentação de pontos de extremidade para que as empresas possam garantir que eles estejam em conformidade com os padrões e normas relevantes do setor, reduzindo o risco de penalidades por não conformidade e fortalecendo sua postura geral de segurança.

Acesso de terceiros: permita que prestadores de serviços e parceiros se conectem a aplicativos específicos sem instalar um agente roteando e autenticando seu acesso através de um portal dedicado da Akamai.

Acesse a página Segurança Zero Trust da Akamai para saber mais