RESUMO DA SOLUÇÃO DA AKAMAI

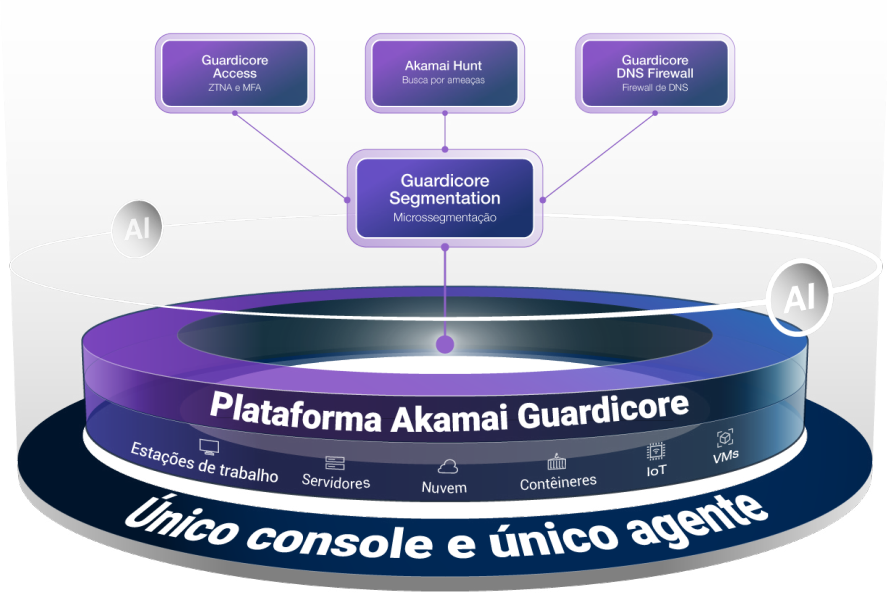
# A Plataforma Akamai Guardicore: Segurança Zero Trust

A implementação do Zero Trust é proibitivamente complexa e cara para a maioria das empresas, especialmente quando essas proteções devem cobrir ativos no local e na nuvem, e uma força de trabalho remota ou no escritório. É por isso que a Plataforma Akamai Guardicore foi criada para lidar de forma eficiente com todas as facetas do Zero Trust com um único console e agente.

À medida que as ciberameaças se tornam cada vez mais sofisticadas e os requisitos regulatórios continuam a ser cada vez mais rigorosos, as organizações enfrentam uma enorme pressão para proteger suas redes e, ao mesmo tempo, manter a eficiência operacional. A Plataforma Akamai Guardicore oferece uma solução Zero Trust abrangente para lidar com esses desafios, fornecendo às organizações as ferramentas e os recursos necessários para implementar um modelo de segurança Zero Trust robusto com eficiência.

A Plataforma Akamai Guardicore foi criada para possibilitar projetos Zero Trust combinando a melhor microssegmentação da categoria, o ZTNA (Zero Trust Network Access), o firewall de DNS e a busca por ameaças em uma plataforma. Juntos, esses componentes simplificam as ações em busca do Zero Trust para reduzir significativamente a superfície de ataque e fortalecer a postura de segurança em toda a empresa.

## A Plataforma Akamai Guardicore




### Microssegmentação

Um dos principais componentes da Plataforma Akamai Guardicore é a microssegmentação. Tradicionalmente, a segurança de rede conta com defesas baseadas em perímetro que se concentram na proteção dos limites externos da rede. No entanto, à medida que as ciberameaças evoluem, fica cada vez mais claro que as defesas de perímetro não são mais suficientes para se proteger contra ataques sofisticados.

## Benefícios

**Infraestrutura consolidada**
Implante rapidamente e escale sem esforço, com impacto mínimo no desempenho.

**Visibilidade abrangente e aprofundada**
Acesse insights abrangentes sobre ativos e comunicações de rede.

**Mecanismo unificado de políticas**
Simplifique a aplicação de políticas em diversos ambientes a partir de uma única interface de usuário.

**Flexibilidade modular**
Aproveite os componentes modulares adaptados às suas necessidades de negócios.

**Cobertura completa**
Proteja todos os seus ativos no local e na nuvem, e os usuários em casa e no escritório.

**As melhores soluções da categoria**
Combine microssegmentação líder do setor e ZTNA para uma postura de segurança aprimorada.

Akamai

A microssegmentação tem uma abordagem diferente dividindo a rede em segmentos menores e mais gerenciáveis e aplicando políticas de segurança a cada segmento com base no princípio do privilégio mínimo. Essa abordagem granular à segurança garante que, mesmo se um segmento for comprometido, o restante da rede permanecerá protegido. Com a Akamai Guardicore Segmentation, cada ativo é protegido, incluindo data centers locais, instâncias de nuvem, sistemas operacionais legados, dispositivos de Internet das coisas, clusters de Kubernetes e muito mais, sem precisar trocar de console.

## Zero Trust Network Access

Além da microssegmentação, a Plataforma Akamai Guardicore também oferece recursos ZTNA (Zero Trust Network Access). ZTNA é um modelo de segurança com base no Zero Trust, o que significa que nenhum usuário ou dispositivo deve ser confiável por padrão, mesmo que esteja dentro da rede corporativa. Em vez disso, o acesso aos recursos é concedido com base na verificação rigorosa de identidade, postura do dispositivo e outros fatores contextuais. Essa abordagem minimiza o risco de acesso não autorizado e ajuda as organizações a evitar violações de dados e ameaças internas.

## Firewall de DNS

Outro componente crítico da Plataforma Akamai Guardicore é o firewall de DNS. O DNS (Sistema de Nomes de Domínio) é um componente fundamental da Internet que converte nomes de domínio legíveis por humanos em endereços IP. No entanto, também é um alvo comum para ataques cibernéticos, já que muitas variantes de malware dependem do DNS para se comunicar com servidores de comando e controle ou para exfiltrar dados. Ao implantar um firewall de DNS, as organizações podem bloquear consultas de DNS mal-intencionadas e impedir que malware se comunique com domínios mal-intencionados, reduzindo assim o risco de violações de dados e outras ciberameaças.

## Busca por ameaças

Por fim, a Plataforma Akamai Guardicore inclui um serviço de segmentação adaptável que permite que as organizações identifiquem e mitiguem de forma proativa as ameaças à segurança antes que elas se agravem e se tornem incidentes completos. A busca por ameaças envolve a busca ativa de sinais de comprometimento dentro da rede, como comportamento anômalo ou IOCs (indicadores de comprometimento). Ao utilizar as ferramentas e técnicas de busca por ameaças, as organizações podem ficar um passo à frente dos invasores e proteger seus ativos valiosos contra danos.

Além de seus principais recursos, a Plataforma Akamai Guardicore também oferece vários benefícios importantes que a diferenciam de outras soluções de segurança no mercado. A plataforma fornece uma infraestrutura leve e consolidada que minimiza a saturação de agentes e a fadiga do console, possibilitando que as organizações implantem e gerenciem sua pilha de segurança com mais eficiência. Além disso, a plataforma oferece visibilidade abrangente e aprofundada dos ativos e das comunicações da rede, possibilitando que os profissionais de segurança recebam insights abrangentes sobre seu ambiente de rede e respondam às ameaças de forma rápida e eficaz.

> No relatório Gartner®, Quick Answer: What Is Zero Trust Networking?, por Andrew Lerner e John Watts, 13 de setembro de 2023, a “Gartner sugere a implementação de microssegmentação e/ou ZTNA para que se avance em direção a uma postura de Rede Zero Trust (ZTN).”*

*GARTNER é uma marca registrada e marca de serviço da Gartner, Inc. e/ou de suas afiliadas nos EUA e internacionalmente, e é usada aqui com permissão. Todos os direitos reservados.

**Visite a página de segurança Zero Trust da Akamai para saber mais.**