RESUMO DO PRODUTO DA AKAMAI

Firewall de DNS da Akamai Guardicore

Visibilidade e controle completos de tráfego de DNS de cargas de trabalho

O DNS (Sistema de Nomes de Domínio) é essencial para serviços de Internet, mas não consegue diferenciar entre solicitações benignas e mal-intencionadas. Consequentemente, as empresas têm implementado firewalls de DNS para inspecionar consultas de DNS, bloquear domínios prejudiciais e resolver domínios seguros. No entanto, como o uso do DNS se estende para abranger cargas de trabalho, servidores e outros dispositivos conectados, a falta de visibilidade e controle desse tráfego de DNS gera outros riscos à segurança.

Unificação entre segmentação e firewall de DNS

A Akamai Guardicore Segmentation, combinada com o Firewall de DNS da Akamai Guardicore, oferece uma defesa poderosa para sua rede. Ao bloquear solicitações de DNS mal-intencionadas e isolar segmentos de rede críticos, essa integração reduz significativamente sua superfície de ataque e impede a disseminação de ameaças. Essa abordagem de camada dupla aumenta a segurança, garante a conformidade e mantém a eficiência operacional, o que a torna uma solução essencial para uma proteção de rede robusta.

Como funciona o Firewall de DNS da Akamai Guardicore

O Firewall de DNS da Akamai Guardicore pode ser ativado em minutos para oferecer segurança e reduzir a complexidade sem afetar o desempenho. Todos os domínios solicitados são verificados pela inteligência contra ameaças em tempo real da Akamai, e as solicitações de domínios mal-intencionados são automaticamente bloqueadas. O uso do DNS como uma camada inicial de segurança bloqueia proativamente as ameaças no início da cadeia de destruição, antes que qualquer conexão com o IP seja feita. Além disso, o DNS foi desenvolvido para ser eficaz na maioria das portas e dos protocolos, garantindo a proteção até mesmo contra malware que não usa as portas e os protocolos padrão da Web.

Quando uma solicitação de DNS é bloqueada, um incidente é criado para fornecer às equipes de segurança e de busca de ameaças informações detalhadas sobre o motivo do bloqueio da ameaça, a origem e o destino da solicitação — que podem ser visualizados em um mapa — e detalhes aprofundados sobre os indicadores de comprometimento.

Benefícios para os seus negócios

Proteção abrangente contra ameaças
Ao filtrar o tráfego de DNS no perímetro da rede e ao aplicar a microssegmentação no nível da rede interna, as empresas podem se defender efetivamente contra tentativas de malware, phishing, comando e controle e exfiltração de dados.

Eficácia aprimorada da busca de ameaças
Os incidentes ajudam as equipes de segurança a detectar, analisar e responder melhor às ameaças emergentes, minimizando o impacto das violações e fortalecendo as defesas gerais de cibersegurança.

Mais visibilidade e contextualização
A combinação entre firewall de DNS e microssegmentação aumenta a visibilidade de padrões de tráfego de DNS para a identificação de possíveis ameaças e violações de políticas.

Gerenciamento simplificado
A combinação entre um firewall de DNS e a microssegmentação simplifica o gerenciamento da segurança através da unificação da criação, da aplicação e do monitoramento de políticas. Isso reduz a complexidade e a sobrecarga operacional, permitindo que as empresas gerenciem sua infraestrutura de segurança com eficiência.

Inteligência de segurança na nuvem da Akamai

O Firewall de DNS da Akamai Guardicore é alimentado pela inteligência de segurança na nuvem da Akamai, que proporciona inteligência em tempo real contra ameaças — e os riscos que essas ameaças representam. A inteligência contra ameaças da Akamai é desenvolvida para oferecer proteção contra perigos atuais e relevantes que possam afetar sua empresa, e para minimizar o número de falsos positivos que suas equipes de segurança precisem investigar. Essa inteligência se baseia em dados coletados 24 horas por dia, 7 dias por semana da Akamai Connected Cloud, que gerencia até 30% do tráfego global da Web e entrega até 14 trilhões de consultas de DNS diariamente. A inteligência da Akamai é reforçada por centenas de feeds externos de ameaças, e o conjunto de dados combinado é continuamente analisado e compilado através de técnicas avançadas de análise comportamental, inteligência artificial e algoritmos patenteados. À medida que novas ameaças são identificadas, elas são adicionadas imediatamente ao conjunto de dados de inteligência contra ameaças para oferecer proteção em tempo real.

Akamai Connected Cloud

O Firewall de DNS da Akamai Guardicore é baseado na Akamai Connected Cloud, a plataforma de computação em nuvem, segurança e entrega de conteúdo mais distribuída do mundo. A Akamai Connected Cloud oferece um acordo de nível de serviço de 100% de disponibilidade e garante confiabilidade otimizada para a segurança de DNS de uma empresa.

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