RESUMO DO PRODUTO DA AKAMAI

Secure Internet Access ThreatAvert

Proteja ativos de rede vitais e identifique ataques de malware que afetam os assinantes

Provedores de serviços reconhecem que a segurança de rede impulsiona o valor da marca, pois afeta diretamente a satisfação dos assinantes. A maioria das ameaças depende de um DNS (Sistema de Nomes de Domínio) para operar, e novas ameaças foram desenvolvidas visando especificamente a infraestrutura crítica de DNS. Os provedores precisam repensar como proteger os assinantes e recursos de rede, especialmente à medida que as ameaças se tornam mais dinâmicas e diversificadas em um mundo onde tudo está conectado.

O Secure Internet Access ThreatAvert da Akamai avalia pesquisas de DNS em tempo real para detectar e interromper atividades mal-intencionadas. O Secure Internet Access ThreatAvert tem como alvo ameaças que causam interrupções ou lentidão na rede, afetam negativamente a experiência dos assinantes ou contornam outras proteções de rede, tais como:

- DDoS com base em DNS que sobrecarrega resolvedores com grandes volumes de consultas
- Ataques de malware por bots que roubam dados pessoais valiosos ou comprometem os dispositivos dos consumidores
- Túneis de DNS que roubam serviços transportando outros protocolos dentro do DNS

O Secure Internet Access ThreatAvert conta com a tecnologia avançada do resolvedor de DNS CacheServe da Akamai, equipado com os feeds de ameaças dinâmicos da Akamai. O CacheServe é o padrão ouro em confiabilidade. Após anos de investimento em otimização de desempenho e inúmeros aprimoramentos de software, a resiliência e a disponibilidade ficam garantidas, mesmo durante grandes picos de tráfego de DNS. A inteligência da Akamai contra ameaças é desenvolvida pela equipe de ciência de dados da Akamai, que processa mais de 100 bilhões de consultas de DNS transmitidas ao vivo de todo o mundo todos os dias.

A segurança de DNS pertence aos servidores de DNS

As consultas de DNS são um dos principais indicadores de atividades mal-intencionadas, pois a resolução do endereço de um recurso mal-intencionado (servidor de comando e controle, download de malware, website de exfiltração etc.) é o primeiro passo para viabilizar a maioria das formas de atividades mal-intencionadas. Os resolvedores de DNS veem todas as consultas em uma rede de provedor. Por isso, uma solução ideal é implementar inteligência nesses locais contra ameaças. A atividade mal-intencionada pode ser detectada pela identificação de consultas recebidas com base em entradas de listas dinâmicas de ameaças.

BENEFÍCIOS PARA SUA EMPRESA

- Solução leve e escalada para milhões de assinantes que abrange todos os dispositivos
- Ciência de dados líder que oferece profundidade e amplitude avançadas de proteção contra ameaças
- Feeds de ameaças atualizados continuamente que mantêm a proteção à medida que as ameaças mudam
- Relatórios em tempo real e fáceis de ler que mostram o status de ameaças rapidamente e o link para os detalhes
- Coleta eficiente e gerenciamento escalável de dados de ameaças e de telemetria

Akamai

O Secure Internet Access ThreatAvert é escalado no plano de controle do DNS, com muito menos custo, esforço operacional e impacto na rede do que as soluções dedicadas de processamento de pacotes, que são escaladas com o tráfego do plano de dados.

É leve e eficiente, e o tráfego de rede não resulta em latência adicional. Como é baseado em rede, todos os dispositivos ficam protegidos, e clientes e hosts não precisam de instalações ou atualizações de software de segurança.

Precisão, profundidade e amplitude avançadas de proteção contra ameaças

Os desenvolvedores de malware inovam continuamente para maximizar o retorno sobre o investimento de suas explorações. Isso significa que a maioria das ameaças é projetada cuidadosamente para que não seja detectada, além de mudar rapidamente para que continue operando. A superfície de ataque também se expandiu e inclui uma variedade impressionante de dispositivos conectados de Internet das coisas. Portanto, há uma diversidade considerável de métodos que os invasores usam para atingir seus objetivos.

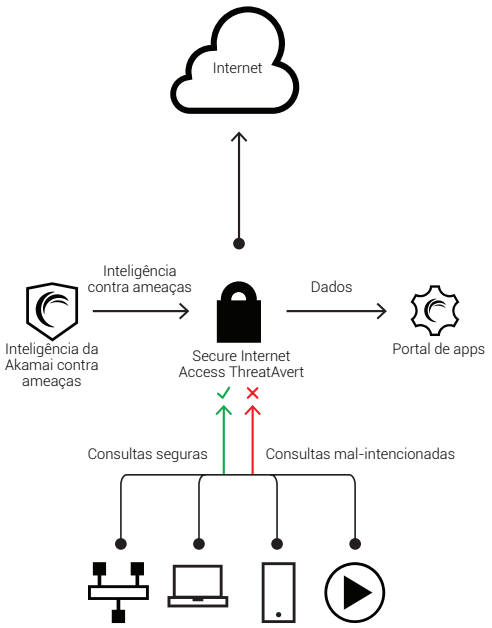
Reconhecendo a sutileza e a diversidade do cenário de ameaças, a equipe de ciência de dados da Akamai desenvolveu, implementou e integrou sistemas fundamentais para analisar consultas de DNS transmitidas ao vivo. Dados de ameaças de listas de reputação, honeypots e outras fontes de terceiros são incorporados ao processo. A amplitude e a profundidade avançadas de proteção, precisão e agilidade contra ameaças são proporcionadas por investimentos em:

- Algoritmos com patente pendente para detectar comportamento anômalo (como DDoS de DNS), correlacionar ameaças díspares e identificar novos algoritmos de geração de domínios de bots instantaneamente
- Técnicas avançadas para permitir nomes automaticamente, garantindo que consultas de DNS "boas" estejam sempre protegidas
- Equipe de pesquisa com anos de experiência em segurança e um profundo conhecimento de dados de malware e DNS
- Rede e data centers mundiais para processamento em tempo real de fluxos de dados ao vivo

Políticas de precisão bloqueiam o tráfego ruim e protegem o tráfego bom

As políticas de precisão são integradas aos feeds de inteligência da Akamai contra ameaças para gerenciar o tráfego de DNS indesejado. Um conjunto amplo e profundo de recursos permite uma filtragem refinada para visar consultas mal-intencionadas e proteger (responder) consultas legítimas:

- As políticas de precisão podem ser aplicadas a consultas recebidas ou respostas enviadas
- Os filtros ou limites de taxa podem ser definidos com base em IP, QTYPE, FQDN ou muitos outros parâmetros de consulta
- Filtros ou limites de taxa podem usar vários parâmetros de consulta juntamente com operadores lógicos: QTYPE E FQDN, IP E FQDN etc.



O grande fluxo de dados processado por especialistas da Akamai oferece uma visão abrangente de atividades mal-intencionadas na Internet, assim como ataques localizados.

- Os filtros ou limites de taxa podem buscar correspondência nas listas dinâmicas da Akamai de inteligência contra ameaças ou em listas fornecidas por operadores
- As políticas e listas de ameaças podem ser combinadas: CORRESPONDÊNCIA na LISTA DE BLOQUEIOS e AUSENTE na LISTA DE PERMISSÕES
- Várias ações de política determinam como as consultas são gerenciadas: descartar, sintetizar resposta, responder com truncamento, NXD, NOERROR e muito mais
- As políticas podem ser combinadas e aninhadas, tornando-as ainda mais eficientes

As políticas de precisão também podem ser configuradas manualmente para resolver problemas localizados em uma rede de provedor.

Gerenciamento de dados escalável, telemetria avançada e geração de relatórios

O Secure Internet Access ThreatAvert apresenta uma arquitetura de gerenciamento de dados com base em soluções abertas de sucesso comprovado nas maiores redes do mundo, oferecendo excelência operacional em escala e velocidade na Web. Os dados transmitidos ao vivo de sistemas Secure Internet Access ThreatAvert em toda a rede são agregados e disponibilizados para a geração de relatórios (descrita abaixo) e outros sistemas. A arquitetura resiliente oferece disponibilidade ininterrupta para proporcionar uma experiência ininterrupta ao cliente. Conectores opcionais para sistemas abertos de Big Data (Splunk, Hadoop) ou aplicações de uso específico podem ser usados para obter insights adicionais de negócios, segurança e operações.

Os relatórios do Secure Internet Access ThreatAvert oferecem uma avaliação instantânea da postura de segurança com um painel executivo que abrange consultas de DNS bloqueadas, recordes registrados de largura de banda de DNS, principais ataques de malware na rede, assinantes infectados e atualizações de inteligência contra ameaças. Um painel de segurança adicional fornece gráficos com detalhes de malware e DDoS. Camadas sucessivas de detalhes sobre malware e clientes infectados também podem ser obtidas com um clique. Relatórios e painéis de controle personalizados podem ser criados em poucos minutos para exibir dados de segurança em um formato definido pelo usuário para atender a requisitos operacionais específicos. Os relatórios baseados em tags permitem que a equipe de operações configure visualizações de sua topologia do Secure Internet Access ThreatAvert para que correspondam aos seus requisitos específicos.