RESUMO DO PRODUTO DA AKAMAI

DNS Posture Management

O DNS (Sistema de Nomes de Domínios) é um componente essencial da infraestrutura de todas as organizações, mas muitas vezes continua sendo uma vulnerabilidade negligenciada. Configurações incorretas e ativos ocultos podem levar a interrupções de serviço, violações de dados e falhas de conformidade, afetando tanto a segurança quanto a continuidade dos negócios.

Uma abordagem proativa para monitoramento, detecção de riscos e aplicação de políticas é crucial para evitar interrupções, reduzir ameaças e garantir a conformidade com as normas do setor e de segurança.

O desafio da segurança de DNS

Atualmente, as organizações enfrentam uma complexidade cada vez maior no gerenciamento de sua postura de DNS devido à evolução das arquiteturas de rede e às implantações híbridas e multinuvem que envolvem vários sistemas de DNS. As empresas lutam para manter a visibilidade em ambientes de rede distribuída onde a TI sombra, as migrações de nuvem e as aquisições criam zonas DNS não documentados e registros que ampliam a superfície de ataque. No lado técnico, as equipes lutam para detectar e corrigir erros de configuração, transferências de zona não autorizadas e higiene de registros desatualizados em plataformas diferentes de DNS.

Sem o monitoramento automatizado, as equipes de segurança dependem de processos manuais que introduzem erros humanos e não conseguem impor políticas de segurança consistentes, deixando a infraestrutura crítica vulnerável a ataques baseados em DNS, incluindo falsificação de DNS, tunelamento e exfiltração de dados. Essa abordagem fragmentada cria riscos significativos de conformidade, ao mesmo tempo em que aumenta o tempo médio para detectar e corrigir problemas, pois as equipes de segurança não dispõem de ferramentas abrangentes que se integram aos centros de operações de segurança existentes.

Como o DNS Posture Management da Akamai ajuda

O DNS Posture Management da Akamai foi projetado para enfrentar esses desafios, fornecendo visibilidade completa, automação e atenuação de riscos para sua infraestrutura de DNS. Ele fornece uma visualização em um único painel consolidando zonas, domínios, subdomínios e registros de todos os provedores de DNS, ajudando a eliminar lacunas de visibilidade e melhorar a eficiência. Essa abordagem centralizada simplifica as complexidades de gerenciar a segurança de DNS em ambientes de vários fornecedores, permitindo que as organizações monitorem, protejam e otimizem sua infraestrutura de DNS a partir de uma única plataforma.

Benefícios para a sua empresa

Rastreie o inventário de DNS
Localize e gerencie ativos de DNS entre provedores com contexto completo de ativos para melhorar a supervisão

Obtenha visibilidade poderosa
Tenha uma visualização em um único painel de seus ambientes de DNS, incluindo AWS Route 53, Akamai Edge DNS, Google Cloud DNS e muito mais

Detecte configurações incorretas
Identifique rapidamente vulnerabilidades e alterações não autorizadas baseadas em configuração que possam comprometer a segurança

Monitore o desvio de DNS
Rastreie alterações não autorizadas ou inesperadas nos registros de DNS, garantindo que as configurações de DNS permaneçam alinhadas às políticas de segurança e às necessidades operacionais da sua organização

Integração perfeita
Os recursos de API sem interface permitem a integração com suas plataformas SIEM, SOAR, GRC, ITSM e XDR favoritas

Proteja sua marca
Identifique e gerencie ameaças de phishing e personificação com monitoramento constante de domínios semelhantes

Mantenha a conformidade contínua
Ajude a atender aos requisitos de conformidade de mais de 15 estruturas (CIS, NIST, ISO, HIPAA, PCI-DSS e muito mais)

Gerencie os certificados
Monitore e avalie os certificados digitais para evitar riscos de segurança, como certificados expirados, configurados incorretamente ou não autorizados

Implante segurança pronta para quantum
Prepare-se para ameaças quânticas com o monitoramento de criptografia pós-quântica (PQC) que ajuda a garantir que sua infraestrutura de certificados permaneça protegida contra futuros ataques quânticos antes que eles se tornem realidade

Transforme a segurança complexa de DNS em inteligência acionável

Uma interface do usuário (IU) avançada com painéis intuitivos permite que os usuários façam uma pesquisa sem obstáculos em todos os principais provedores de DNS, visualizando relacionamentos e possíveis ameaças (Figura 1). Os alertas são priorizados por gravidade, o que garante que os problemas críticos recebam atenção imediata. Os recursos de monitoramento em tempo real detectam riscos emergentes, incluindo desvio de DNS, que pode indicar comprometimento da configuração, além de identificar domínios semelhantes e typosquatting, que têm como alvo a sua marca.

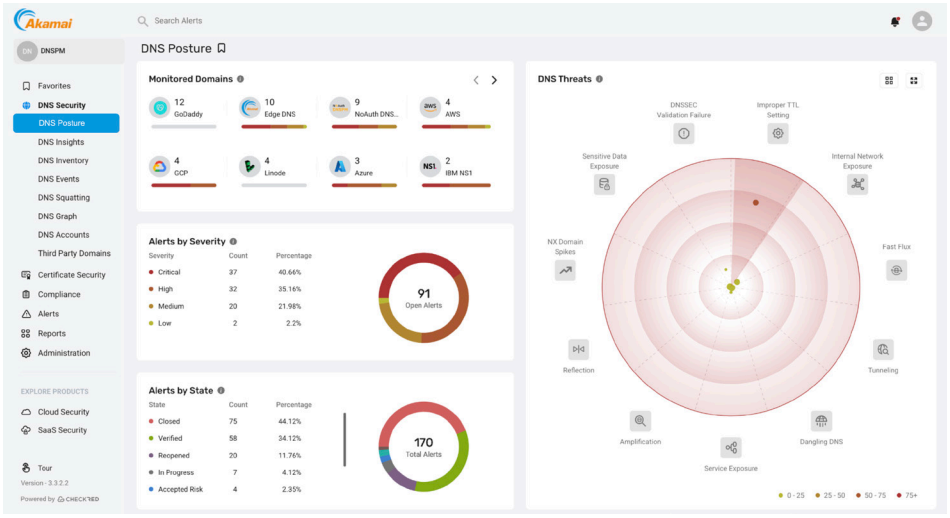

Fig. 1: o painel avançado fornece visibilidade completa e controle sobre os ativos de DNS para detectar e corrigir ameaças e configurações incorretas

A interface do usuário também oferece um valioso recurso de benchmarking do setor, que fornece pontuação de risco comparativa em relação a dados anônimos de empresas semelhantes, ajudando as empresas a quantificar sua postura de segurança de DNS em relação a seus pares (Figura 2).

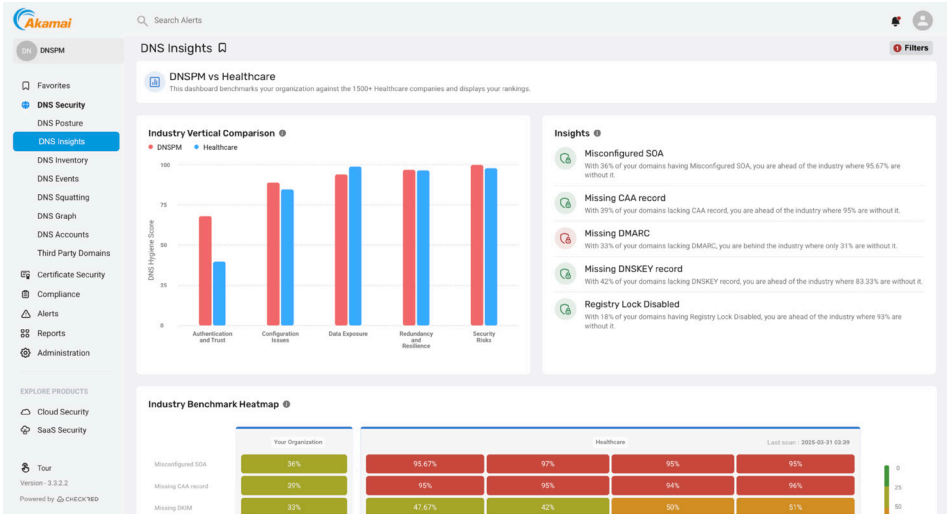

Fig. 2: as organizações podem comparar sua postura de segurança à de pares do setor

Principais recursos

Cobertura de vários provedores

- Ele se integra perfeitamente a todos os principais provedores de DNS, incluindo Akamai Edge DNS, AWS Route 53, Azure DNS, Infoblox, Google Cloud DNS e muito mais, para uma segurança consistente e um controle centralizado

Visibilidade unificada de todos os ambientes

- Ele oferece uma visualização em um único painel de todos os ativos de DNS (domínios, subdomínios e registros), abrangendo vários provedores de nuvem e infraestruturas locais

Verificações detalhadas de políticas

- Realize verificações de políticas e configurações abrangentes em toda a sua infraestrutura de DNS, incluindo a detecção de danglers do CNAME, para descobrir vulnerabilidades antes que elas possam ser exploradas; aplique regras extensíveis para adaptar as verificações de segurança de DNS às políticas exclusivas da sua organização e às necessidades de conformidade em constante evolução

Detecção e prevenção proativas de riscos

- Não requer instalação em pontos de extremidade ou servidores, oferecendo implantação rápida, sobrecarga mínima e informações imediatas das vulnerabilidades

Geração de relatórios e fluxos de trabalho de correção dinâmica

- Ele fornece orientações passo a passo de correção com fluxos de trabalho manuais, semiautomatizados e totalmente automatizados, facilitando a resolução de problemas de forma rápida e eficaz

Manutenção da conformidade

- Ajuda as organizações a manter a conformidade (seguindo os benchmarks do CIS [Center of Internet Security]), reduzir o risco regulatório e manter a confiança do cliente por meio de verificações contínuas de políticas e relatórios abrangentes

Gerenciamento da postura de certificados

- Identifique certificados TLS/SSL configurados incorretamente ou expirados para reduzir a exposição e dar suporte à prontidão para auditoria

Akamai Managed Service (opcional)

- Os especialistas do SOCC monitoram ativamente sua infraestrutura de DNS para fornecer recomendações proativas relacionadas a vulnerabilidades e oferecer suporte de emergência para ameaças detectadas

Para saber mais, acesse akamai.com/pt/ ou entre em contato com sua equipe de vendas da Akamai.