FICHE PRODUIT AKAMAI

DNS Posture Management

Le DNS (système de noms de domaine) est un composant essentiel de l'infrastructure de toute entreprise, et pourtant il représente une vulnérabilité souvent négligée. Les erreurs de configuration et les ressources cachées peuvent entraîner des interruptions de service, des violations de données et des échecs de conformité, ce qui a un impact sur la sécurité et la continuité de l'activité.

Une approche proactive de la surveillance, de la détection des risques et de l'application des règles est cruciale pour prévenir les pannes, atténuer les menaces et assurer la conformité aux réglementations du secteur et de la sécurité.

L'enjeu de la sécurité DNS

Aujourd'hui, la gestion de la stratégie DNS des entreprises devient de plus en plus complexe en raison de l'évolution des architectures réseau et des déploiements hybrides et multicloud qui impliquent plusieurs systèmes DNS. Les entreprises peinent à maintenir une visibilité sur tous les environnements réseau distribués, où l'activité informatique fantôme, les migrations vers le cloud et les acquisitions créent des zones et des enregistrements DNS non documentés qui étendent la surface d'attaque. Sur le plan technique, les équipes sont aux prises avec la détection et la correction des erreurs de configuration, les transferts de zone non autorisés et la gestion des enregistrements obsolètes dans l'ensemble des plateformes DNS disparates.

Sans surveillance automatisée, les équipes de sécurité doivent se contenter de processus manuels, qui peuvent occasionner des erreurs humaines et n'aident pas à assurer la cohérence des stratégies de sécurité. Cela rend l'infrastructure critique vulnérable aux attaques DNS, notamment l'usurpation de DNS, la tunnellisation et l'exfiltration de données. Les équipes de sécurité ne disposant pas d'outils complets qui s'intègrent aux centres d'opérations de sécurité existants, cette approche fragmentée conduit à d'importants risques de conformité tout en augmentant le temps moyen de détection et de résolution des problèmes.

Comment la solution Akamai DNS Posture Management peut-elle vous aider ?

La solution Akamai DNS Posture Management est conçue pour prendre ces défis à bras-le-corps en fournissant une visibilité de bout en bout, une automatisation et une atténuation des risques pour votre infrastructure DNS. Elle offre une vue d'ensemble unique en consolidant les zones DNS, les domaines, les sous-domaines et les enregistrements de tous les fournisseurs DNS, afin de combler les lacunes en matière de visibilité et d'améliorer l'efficacité. Cette approche centralisée simplifie la gestion de la sécurité DNS dans les environnements multifournisseurs, ce qui permet aux entreprises de surveiller, sécuriser et optimiser leur infrastructure DNS à partir d'une seule plateforme.

Avantages pour votre entreprise

Suivi de l'inventaire DNS
Localisez et gérez les ressources DNS de l'ensemble des fournisseurs grâce à des informations complètes sur les ressources, pour une surveillance optimale

Visibilité accrue
Bénéficiez d'une vue d'ensemble unique sur tous vos environnements DNS, y compris AWS Route 53, Akamai Edge DNS, Google Cloud DNS et bien d'autres

Détection des erreurs de configuration
Identifiez et résolvez rapidement les vulnérabilités liées à la configuration et les modifications non autorisées susceptibles de compromettre la sécurité

Surveillance des dérives DNS
Suivez les modifications non autorisées ou inattendues apportées aux enregistrements DNS, afin de vous assurer que les paramètres DNS restent alignés sur les stratégies de sécurité et les besoins opérationnels de votre entreprise

Intégration fluide
Des fonctionnalités d'API sans interface permettent l'intégration à vos plateformes SIEM, SOAR, GRC, ITSM et XDR préférées

Protection de votre marque
Identifiez et gérez les menaces d'hameçonnage et d'usurpation d'identité grâce à une surveillance continue des domaines similaires

Maintien de la conformité
Assurez votre conformité à plus de 15 cadres réglementaires (CIS, NIST, ISO, HIPAA, PCI-DSS, et plus encore)

Gestion des certificats
Surveillez et évaluez les certificats digitaux pour éviter les risques de sécurité liés aux certificats expirés, mal configurés ou indésirables

Déploiement d'une défense contre les attaques quantiques
Préparez-vous à faire face aux menaces quantiques grâce à la surveillance de la cryptographie post-quantique (PQC), qui vous permet d'assurer la protection de votre infrastructure de certificats contre toute attaque quantique potentielle

Transformer la complexité de la sécurité DNS pour en tirer des informations exploitables

Les utilisateurs bénéficient d'une puissante interface utilisateur (UI) dotée de tableaux de bord intuitifs, afin d'effectuer des recherches de manière fluide sur tous les principaux fournisseurs DNS, et peuvent visualiser les relations et les menaces potentielles (Figure 1). Les alertes sont classées par gravité, ce qui permet une intervention immédiate sur les problèmes critiques. Les fonctionnalités de surveillance en temps réel détectent les risques émergents, notamment les dérives DNS qui peuvent indiquer une compromission de la configuration, tout en identifiant les domaines similaires et le typosquatting qui ciblent votre marque.

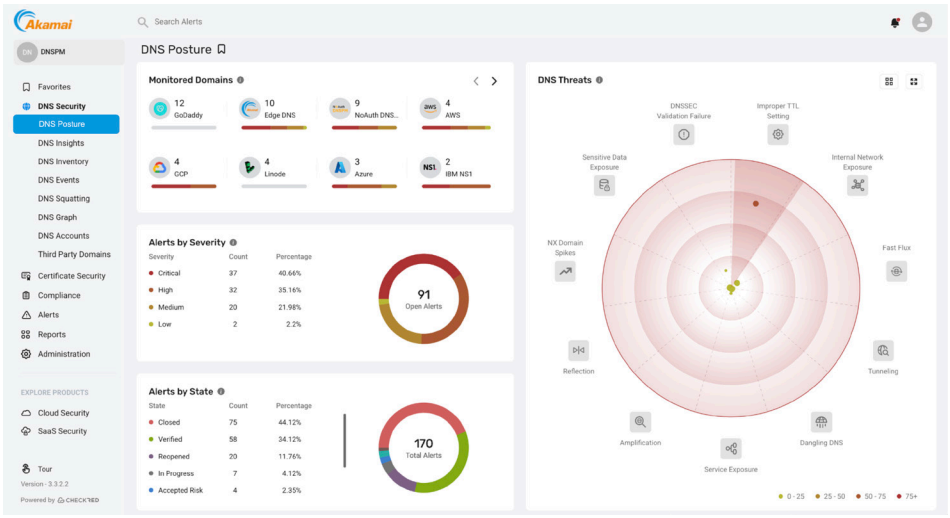

Fig. 1 : Un tableau de bord puissant qui offre une visibilité et un contrôle complets sur les ressources DNS, pour détecter et corriger les menaces et les erreurs de configuration

L'interface utilisateur propose également une fonction d'analyse comparative du secteur, qui fournit une évaluation comparative des risques par rapport aux données anonymisées d'entreprises similaires, aidant ainsi les entreprises à mesurer leur stratégie de sécurité DNS par rapport à leurs pairs (Figure 2).

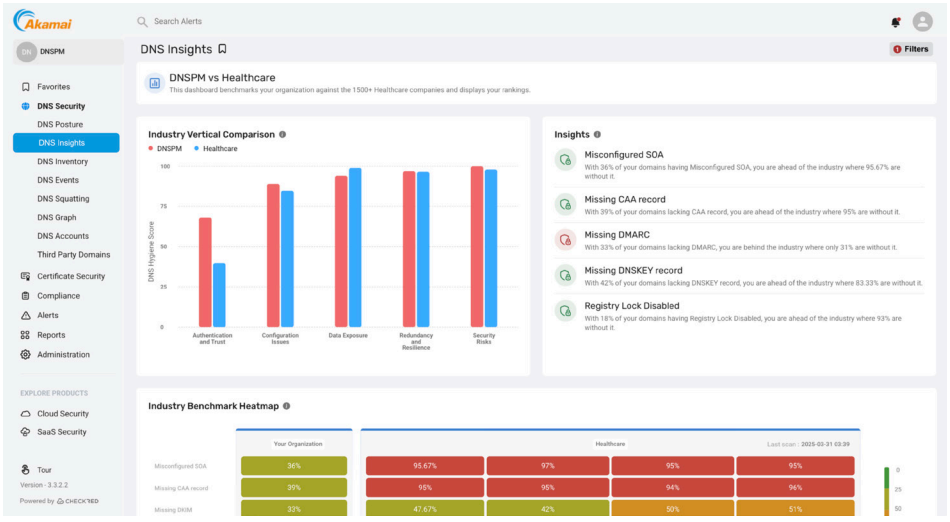

Fig. 2 : Les entreprises peuvent comparer leur stratégie de sécurité à celle de leurs homologues du secteur

Principales fonctionnalités

Couverture multifournisseur

- S'intègre parfaitement avec les principaux fournisseurs DNS, notamment Akamai Edge DNS, AWS Route 53, Azure DNS, Infoblox, Google Cloud DNS, et bien plus encore, pour une sécurité cohérente et un contrôle centralisé

Visibilité unifiée sur l'ensemble des environnements

- Offre une vue granulaire de toutes les ressources DNS (domaines, sous-domaines et enregistrements) disponibles sur plusieurs fournisseurs de cloud et infrastructures sur site

Vérifications des règles en profondeur

- Effectue des vérifications en profondeur des règles et configurations de votre infrastructure DNS (y compris la détection des enregistrements CNAME orphelins) pour identifier les vulnérabilités avant qu'elles ne puissent être exploitées. Applique des protocoles extensibles pour adapter les vérifications de sécurité DNS aux règles uniques de votre organisation et aux besoins en matière de conformité qui ne cessent d'évoluer

Détection et prévention proactives des risques

- Ne nécessite aucune installation sur les points de terminaison ou les serveurs, assurant un déploiement rapide, des frais peu élevés et une visibilité immédiate sur les vulnérabilités

Flux de travail et rapports de mesures correctives dynamiques

- Fournit des instructions pas à pas pour l'application de mesures correctives avec des flux de travail manuels, semi-automatisés et entièrement automatisés, ce qui favorise une résolution rapide et efficace des problèmes

Maintien de la conformité facilité

- Aide les entreprises à maintenir la conformité (d'après les benchmarks CIS [Center for Internet Security]), à réduire les risques réglementaires et à préserver la confiance des clients grâce à des contrôles continus des règles et à des rapports complets

Certificate Posture Management

- Identifie les certificats TLS/SSL mal configurés ou expirés pour réduire l'exposition et se préparer aux audits

Akamai Managed Service (en option)

- Les spécialistes du centre de commande des opérations de sécurité surveillent activement votre infrastructure DNS afin d'offrir des recommandations proactives pour résoudre les vulnérabilités et de fournir une assistance d'urgence en cas de menaces détectées

Pour en savoir plus, rendez-vous sur akamai.com ou contactez votre équipe commerciale Akamai.

| Publication : 06/25