FICHE TECHNIQUE

Infoblox Threat Defense™ Advanced

DNS protecteur, alimenté par une Threat Intelligence prédictive, protège tout, partout, avant l'impact

LE DNS EST LE PREMIER POINT DE PRÉVENTION CONTRE TOUTES LES CYBERATTAQUES

Le DNS est le premier point de détection et de prévention de toutes les cyberattaques. Qu'il s'agisse d'un e-mail de phishing, d'un texte de smishing ou d'une vulnérabilité exploitée, presque toutes les attaques génèrent une requête DNS vers un domaine malveillant. Par conséquent, le DNS fournit un point de visibilité et de contrôle puissant et centralisé pour sécuriser l'ensemble d'une entreprise, y compris les utilisateurs, les appareils, l'IoT/OT et les charges de travail, que ce soit sur site, dans le cloud ou à la périphérie.

En tant que première étape de toute communication, la détection et le blocage des activités malveillantes au niveau DNS permettent d'arrêter le trafic malveillant avant qu'il n'atteigne les outils en aval et ne déclenche des alertes. En corrélant les données DNS avec le contexte des appareils et des actifs, les équipes NetOps et SecOps bénéficient d'une visibilité accrue sur ce qui se passe dans leurs environnements, ce qui améliore à la fois l'efficacité opérationnelle et la posture de sécurité.

LES SOLUTIONS TRADITIONNELLES DE « DÉTECTION ET RÉPONSE » NE SONT PLUS EFFICACES

Les acteurs de la menace utilisent de plus en plus l'intelligence artificielle pour lancer des campagnes plus prolifiques, plus sophistiquées et plus furtives. Ils génèrent des malwares à usage unique, conçus de manière unique, qui rendent inefficaces les outils traditionnels de « détection et réponse », c'est-à-dire ceux qui attendent une infection « patient zéro ». Chaque attaque se transforme en un scénario de « patient zéro » où il n'existe aucune signature ou comportement connu. Les outils de « détection et de réponse » agissent souvent trop tard dans la chaîne de destruction pour éviter les dommages. Une approche préventive différente est donc nécessaire. Un dispositif qui arrête les menaces avant qu'elles ne pénètrent dans l'environnement ou ne se déplacent latéralement. Ceci permet non seulement de bloquer les attaques plus tôt, mais également de réduire la charge sur les outils traditionnels de « détection et de réponse ».

Le DNS fonctionne comme un point de contrôle en amont, offrant aux équipes de sécurité une opportunité proactive de détecter et de bloquer les menaces plus tôt, avant qu'elles n'atteignent les utilisateurs, les charges de travail ou les terminaux.

LA SÉCURITÉ PRÉVENTIVE AVEC LE DNS

Infoblox Threat Defense™ Advanced offre une **approche préventive** unique à la détection des menaces. Une approche qui ne repose pas sur le « patient zéro ». Elle associe une combinaison de **threat intelligence prédictive** qui bloque l'infrastructure des acteurs malveillants avant qu'ils ne soient utilisés comme armes, à une analyse algorithmique et automatique des requêtes DNS sur les réseaux clients pour assurer une protection avant tout impact. Grâce à l'identification rapide des actifs impliqués dans les incidents de sécurité, à l'intégration de l'écosystème et à des espaces de travail intuitifs, elle permet une détection et une réponse plus rapides, ainsi qu'une optimisation du retour sur investissement (ROI) de vos solutions de sécurité existantes.

DES FAITS ET DES CHIFFRES

- Surveille **204 000** clusters d'acteurs de menace en temps réel, un nombre en constante augmentation
- Réduit le taux de faux positifs à **0,0002 %**
- Bloque **82 %** des menaces avant la première requête
- Offre une protection **68,4** jours avant une attaque en moyenne
- Bloque **5 fois plus** de domaines à haut risque/moyen risque que les outils qui se contentent de rechercher les comportements malveillants connus.
- Permet d'économiser en moyenne **500 heures d'analyste SOC** par mois*
- Permet de réaliser **400 000 $** d'économies de productivité par an*
- Réduit des dizaines de milliers d'alertes à une poignée*

L'enquête SOC 2025 de SANS a révélé que sept des 10 principaux obstacles à la pleine utilisation des SOC concernent les alertes, l'intégration des outils et la pénurie de compétences.

* Basé sur des données client réelles.

LE BLOCAGE DES MENACES AVANT IMPACT

Infoblox Threat Defense applique la threat intelligence DNS prédictive avec des analyses algorithmiques et d'apprentissage automatique sur le trafic DNS en temps réel afin de bloquer les activités liées aux menaces avant qu'elles n'affectent votre réseau, détectant souvent des menaces que d'autres outils ne parviennent pas à détecter. En bloquant les menaces au niveau DNS, Infoblox permet également de réduire le volume d'alertes et la charge de travail des outils de sécurité en aval, avec des clients constatant jusqu'à 50 % de réduction des alertes sur les pare-feux nouvelle génération (NGFW) et les systèmes de détection et de réponse des endpoints (EDR).

> *« Un DNS sécurisé pourrait réduire la capacité de 92 % des attaques de malwares à déployer avec succès des malwares sur un réseau donné. »*
>
> **Anne Neuberger,**
> **Directeur de la cybersécurité Direction,**
> **Agence de sécurité nationale (NSA)**

Capacité clé	Description	Infoblox Threat Defense	NGFW	SASE	EDR
Résolveur sécurisé à l'échelle de l'entreprise et journalisation des requêtes DNS	Utilise les données de requête DNS pour identifier et signaler des domaines	●	◑	◑	◑
Surveillance complète du comportement DNS	Surveille tous les types d'enregistrements DNS pour détecter des activités malveillantes	●	●	◔	○
Détection et suppression des domaines similaires/ Doppleganger	Réduction de la surface d'attaque des domaines similaires/usurpés	●	○	◑	○
Protection DNS Zero-Day	Identifie les domaines nouveaux ou émergents liés à votre entreprise qui pourraient représenter une menace	●	◑	◑	○
Détection du Tunneling DNS basée sur le comportement	Détecte les tunnels DNS utilisés pour l'exfiltration/infiltration de données, les communications C2, etc.	●	◑	◑	○
Protection proactive des domaines suspects ou à haut risque	Identifie et bloque de manière préventive les domaines à risque susceptibles d'être utilisés dans de futures campagnes malveillantes	●	◑	◑	◑
Enrichissement contextuel automatique et natif	Corrèle le contexte réseau sans nécessiter de clients ni de redirection de trafic (utilisateur, appareil, IP source, emplacement, adresse MAC, VLAN)	●	◑	◑	◑
Détection et perturbation proactive des systèmes de distribution de menaces (TDS)	Identifie l'infrastructure TDS des acteurs malveillants, et pas seulement les domaines individuels, afin de contrer les acteurs malveillants qui passent d'un domaine à l'autre pour échapper à la détection.	●	◔	○	○

Figure 1. Possibilités uniques de Threat Defense que d'autres outils ne peuvent pas offrir

LES FONCTIONNALITÉS CLÉS DE THREAT DEFENSE

- **Surveillance « Protection avant impact ».** Permet aux RSSI et aux équipes de sécurité de mettre en œuvre une stratégie préventive et de rendre compte en toute confiance au comité de direction, grâce à des indicateurs clairs et quantifiables sur les menaces neutralisées avant impact, — offrant un gain de temps crucial et réduisant la charge du centre des opérations de sécurité (SOC).
- **Découverte des actifs et intégration de l'inventaire.** Identification rapide des actifs impliqués dans les incidents de sécurité pour une évaluation et une réponse plus rapides.
- **Espace de travail sécurité.** Une interface simplifiée et intuitive qui permet aux équipes de sécurité de comprendre clairement ce qui se passe dans leur environnement et de proposer des moyens de réduire les risques.
- **Mode de détection.** Déploiement simple et une validation du concept sans modifier l'infrastructure informatique ou réseau existante.

LA SÉCURITÉ PRÉVENTIVE RENFORCÉE PAR UNE INTELLIGENCE PRÉDICTIVE

Infoblox est le principal créateur de la Threat Intelligence DNS. L'entreprise adopte une approche préventive, et pas seulement défensive, en utilisant ses connaissances pour suivre l'infrastructure des acteurs de la menace au fur et à mesure de sa construction et pour perturber la cybercriminalité à la source, souvent avant même qu'une attaque ne soit lancée.

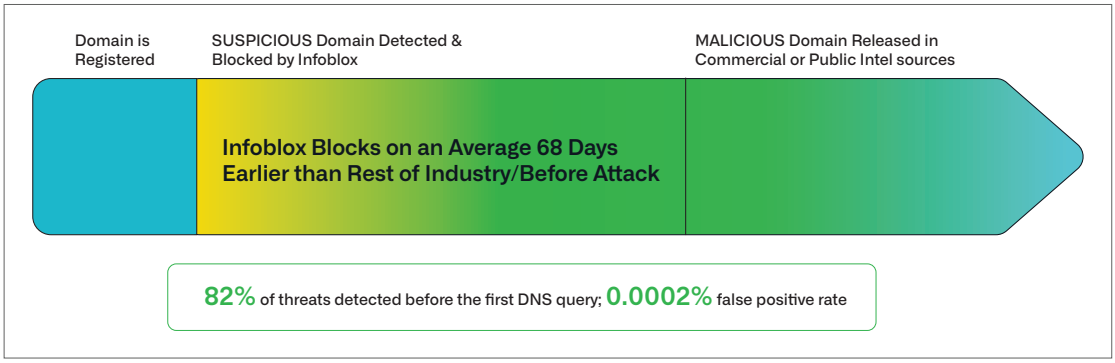

Figure 2. Infoblox Threat Intelligence peut protéger contre les menaces avant le reste du secteur de la sécurité.

Création par Infoblox d'une Threat Intelligence DNS exclusive

Experts DNS : Infoblox découvre les acteurs de la menace qui se cachent dans le DNS en sachant où chercher. En commençant par les domaines à haut risque ou suspects, l'équipe relie les points pour identifier l'infrastructure de l'attaquant et la suivre au fur et à mesure qu'elle évolue et fait apparaître de nouvelles menaces, avant qu'elles ne soient reconnues ailleurs.

Expertise en menaces : Infoblox comprend comment les acteurs malveillants opèrent et comment se manifestent les menaces telles que les malwares, les ransomwares, le phishing et les exploits basés sur DNS. Cette expertise alimente les systèmes prédictifs qui détectent les domaines similaires, l'activité de commande et de contrôle (C2) DNS, les registered domain generation algorithms (RDGAs) et d'autres comportements suspects.

Science des données : Infoblox applique l'apprentissage automatique et la data science avancée à des volumes massifs de données de requêtes DNS. Cela permet une protection en temps quasi réel contre l'Exfiltration de données, les algorithmes de génération de domaines (DGA) et un large éventail de menaces évasives.

L'OPTIMISATION DE LA SÉCURITÉ AVEC SOC INSIGHTS

Qu'il s'agisse de la surcharge d'alertes, de l'épuisement des analystes ou de la longueur des enquêtes et des réponses, Infoblox Threat Defense apporte un soulagement concret au SOC grâce au module SOC Insights.

- Aidez les analystes à savoir ce qui compte le plus grâce à des analyses basées sur l'IA qui ramènent des centaines de milliers d'alertes à une poignée d'informations.
- Automatisez la journalisation, la threat intelligence et d'autres tâches de collecte et de corrélation des données afin que les analystes puissent démarrer rapidement leurs investigations et leurs interventions.
- Accélérez la réponse aux incidents grâce à la découverte des ressources et à l'intégration de l'inventaire, aidant les analystes à identifier plus rapidement les appareils impactés.

Figure 3. Infoblox Threat Intel a partagé des données de recherche surprenantes sur le risque croissant des domaines similaires.

L'EXPORTATION DE JOURNAUX DNS DE HAUTE VALEUR À GRANDE ÉCHELLE

Infoblox facilite l'envoi de données de requêtes et d'événements DNS de haute fidélité à votre SIEM, SOAR ou data lake pour une visibilité centralisée et une corrélation plus rapide des menaces.

- Filtrez et transmettez uniquement les événements DNS de grande valeur afin de réduire les coûts d'ingestion SIEM et le bruit des alertes.
- Diffusez des journaux DNS enrichis en temps réel à l'aide de l'Infoblox Cloud Data Connector.
- Améliorez la détection et la réponse dans tout votre écosystème en fournissant à chaque outil le contexte nécessaire.
- Partagez des données de manière fluide avec d'autres outils grâce à des intégrations bidirectionnelles certifiées, améliorant ainsi la détection, le triage et la réponse de bout en bout.

ENQUÊTEZ PLUS RAPIDEMENT AVEC DOSSIER

Dossier fournit aux analystes un outil de recherche puissant et unifié pour valider les menaces, pivoter sur les IOC ou Indicateurs de compromission et accélérer les enquêtes, sans avoir besoin de basculer entre différentes plates-formes.

- Consolidez la Threat Intelligence interne, Infoblox et tierces dans une interface intuitive unique.
- Enquêtez rapidement sur les IOC et découvrez les menaces associées grâce à l'enrichissement intégré et à l'analyse des liens.
- Réduisez le temps d'investigation jusqu'à 67 % en éliminant la collecte manuelle des données et le changement de contexte.

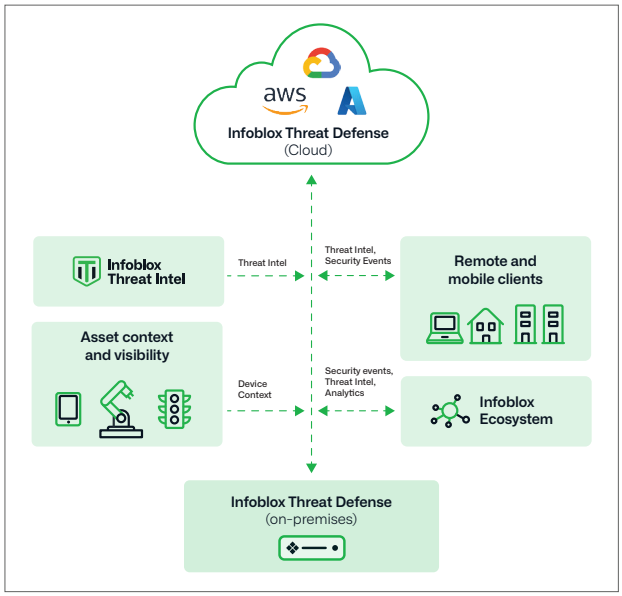

Figure 4. L'architecture hybride d'Infoblox permet une protection et un déploiement n'importe où pour contrer le paysage actuel des menaces basées sur l'IA.

PROTÉGEZ VOTRE MARQUE CONTRE LA DÉCEPTION CIBLÉE

Infoblox propose deux fonctionnalités intégrées : la surveillance des domaines similaires et les services de mitigation des domaines, qui vous aident à protéger votre marque, vos clients et vos employés contre les cyberattaques basées sur la déception. Ensemble, ils vous offrent une visibilité sur les menaces émergentes et vous permettent de prendre des mesures rapides et efficaces contre les domaines malveillants avant qu'ils n'impactent votre activité.

Surveillance de domaines similaires

Gardez une longueur d'avance sur les attaques d'usurpation d'identité qui exploitent votre marque ou des tiers de confiance.

- Détectez les domaines enregistrés pour usurper l'identité de votre entreprise, de votre chaîne d'approvisionnement ou de vos propriétés orientées client.
- Identifiez les domaines utilisés dans les campagnes de phishing et de fraude visant vos employés ou vos clients.
- Surveillez les domaines hautement prioritaires pour détecter les changements de posture de risque et recevez des alertes en temps réel.

Services de mitigation de domaines

Validez et supprimez rapidement les domaines malveillants actifs dans la nature.

- Confirmez et documentez les activités malveillantes grâce à une validation des incidents menée par des humains et à des rapports de synthèse.
- Coordonnez-vous avec les FAI mondiaux, les hébergeurs et les autorités réglementaires pour un retrait rapide, souvent dans les 24 heures.
- Surveillez les menaces atténuées pendant 30 jours après la suppression pour détecter et supprimer les tentatives de réactivation sans frais supplémentaires.
- Traitez une série de types de menaces, notamment le phishing, l'hébergement de malwares, l'infrastructure C2 et les données volées.

Pour en savoir plus sur la manière dont Infoblox Threat Defense sécurise vos données et votre infrastructure, veuillez consulter https://www.infoblox.com/fr/products/threat-defense/.

Siège social
2390 Mission College Boulevard,
Ste. 501 Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/fr

Version : 20250121v1