FICHE TECHNIQUE

Infoblox Threat Defense™

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

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

Qu'il s'agisse d'un e-mail de phishing, un SMS de smishing ou une vulnérabilité exploitée, presque toutes les attaques génèrent une requête DNS vers un domaine malveillant. Par conséquent, le DNS offre un point de visibilité et de contrôle puissant et centralisé pour l'ensemble de l'entreprise (utilisateurs, appareils, IoT/OT et charges de travail) que ce soit sur site, dans le cloud ou à la périphérie.

Le DNS est impliqué dans presque toutes les interactions numériques, en faisant un point de contrôle idéal pour la prévention précoce des menaces. En inspectant le trafic DNS en temps réel, Infoblox peut détecter et bloquer les activités malveillantes avant qu'elles n'atteignent les outils en aval ou ne génèrent des alertes. Lorsqu'elles sont mises en corrélation avec le contexte des actifs et des identités, les données DNS offrent aux équipes NetOps et SecOps une visibilité renforcée sur leurs environnements, améliorant l'efficacité opérationnelle et la posture de sécurité.

Les acteurs malveillants exploitent de plus en plus l'IA pour mener des campagnes plus prolifiques, sophistiquées et furtives. Ils génèrent des malwares à usage unique, conçus de façon unique, rendant inefficaces les outils traditionnels de « détection et réponse », c'est-à-dire ceux qui attendent une infection « patient zéro ». Chaque attaque devient un scénario de « patient zéro », sans qu'aucune signature ni comportement connus n'existent. Ces outils interviennent souvent trop tard dans la chaîne d'attaque pour prévenir les dommages.

Une approche préventive est nécessaire, c'est-à-dire une méthode qui stoppe les menaces avant qu'elles ne pénètrent dans l'environnement ou ne se déplacent latéralement. Le DNS offre aux équipes de sécurité la possibilité de détecter et de bloquer les menaces de manière proactive, avant qu'elles n'atteignent les utilisateurs, les charges de travail ou les endpoints.

LA SÉCURITÉ PRÉVENTIVE GRÂCE AU DNS

Infoblox Threat Defense™ offre une **approche préventive** unique pour la détection des menaces, c'est-à-dire une approche qui ne repose pas sur le « patient zéro ». Elle combine une **threat intelligence prédictive** capable de bloquer l'infrastructure des acteurs malveillants avant qu'elle ne soit utilisés comme armes, avec une analyse algorithmique et automatisée des requêtes DNS sur les réseaux clients, garantissant 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, tout en optimisant le retour sur investissement (ROI) de vos solutions de sécurité existantes.

La solution Threat Defense, alimentée par la threat intelligence prédictive basée sur le DNS, permet aux équipes de sécurité d'identifier l'infrastructure des attaquants avant qu'elle ne soit utilisée comme arme et d'anticiper la chaîne d'attaque. Elle partage également le contexte des menaces et des actifs au sein de votre écosystème de sécurité, améliorant la précision et l'efficacité de l'ensemble de votre pile de sécurité.

DES FAITS ET DES CHIFFRES

- Surveille **204 000** clusters d'acteurs malveillants 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
- Économise en moyenne **500 heures de travail** par mois* **pour les analystes SOC**
- Permet de réaliser **400 000 $** d'économies liées à la productivité par an*
- Réduit des dizaines de milliers d'alertes à seulement une poignée*

L'enquête SANS 2025 SOC a révélé que sept des dix principaux obstacles empêchant 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 L'IMPACT

Threat Defense applique la threat intelligence DNS prédictive et des analyses algorithmiques et d'apprentissage automatique sur le trafic DNS en temps réel afin de bloquer les activités malveillantes avant qu'elles n'affectent votre réseau, détectant souvent des menaces que d'autres outils ne parviennent pas à identifier. 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, les 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 de 92 % la réussite des attaques de malware 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
Serveur de résolution 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 nouveaux domaines ou ceux en émergence liés à votre entreprise qui pourraient constituer une menace.	●	◑	◑	○
Détection du DNS Tunneling 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 de la menace 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

- **Moniteur « Protection avant impact » :** Permet aux CISO et aux équipes de sécurité de mettre en œuvre leur stratégie de sécurité 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.
- **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 efficaces.
- **Espace de travail sécurité :** Une interface simplifiée et intuitive qui permet aux équipes de sécurité de visualiser clairement leur environnement et de proposer des moyens de réduire les risques.
- **Mode de détection :** Déploiement simple et validation du concept sans modification de l'infrastructure informatique ou réseau existante.

LA SÉCURITÉ PRÉVENTIVE RENFORCÉE GRÂCE À L'INTELLIGENCE PRÉDICTIVE

Infoblox est le leader de la threat intelligence basé sur le DNS.L'entreprise adopte une approche préventive, et non seulement défensive, en utilisant ses connaissances pour suivre l'infrastructure des acteurs de la menace au fur et à mesure de sa création et pour arrêter la cybercriminalité à la source, souvent avant même qu'une attaque ne soit lancée.

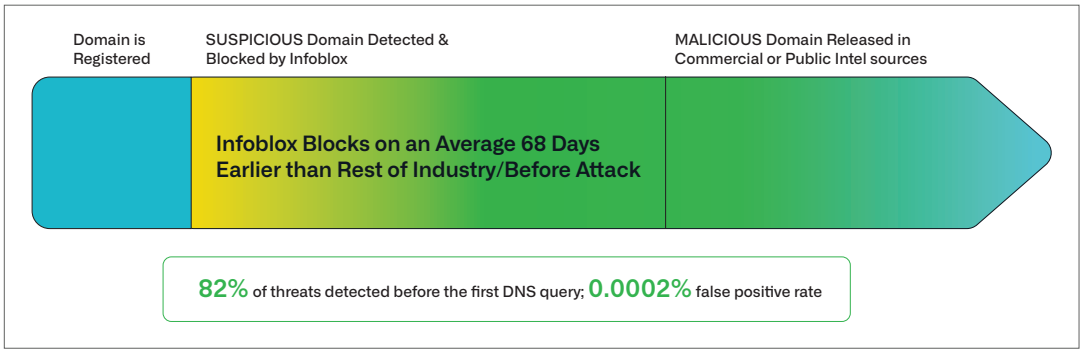

Figure 2. Infoblox Threat Intelligence peut protéger contre les menaces avant le reste du secteur de la sécurité

Comment Infoblox crée des informations inédites sur les menaces DNS ?

Experts DNS : Infoblox détecte les acteurs malveillants qui se cachent dans le DNS en déterminant où il faut chercher. En commençant par les domaines à haut risque ou suspects, l'équipe établit des liens pour identifier l'infrastructure des attaquants, suit chaque évolution et détecte les nouvelles menaces avant qu'elles ne soient identifiées ailleurs.

Expertise en menaces : Infoblox comprend le fonctionnement des acteurs malveillants et la manière dont se manifestent les menaces, telles que les malwares, ransomwares, phishing et exploits basés sur DNS. Cette expertise alimente les systèmes prédictifs qui détectent les domaines similaires, l'activité de commande et de contrôle DNS, les algorithmes de génération de domaines enregistrés (RDGA) et d'autres comportements suspects.

Science des données : Infoblox applique un 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.

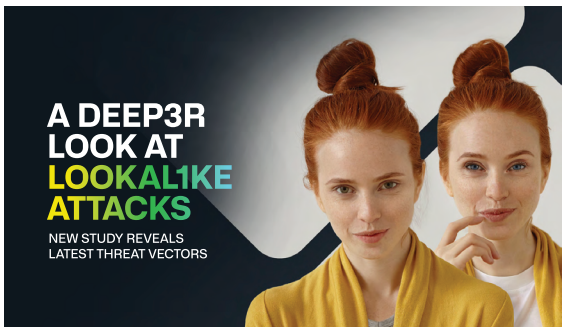

Figure 3. Infoblox Threat Intel a partagé des données de recherche surprenantes sur le risque croissant lié aux domaines 'Lookalike'.

LES FORFAITS DE SÉCURITÉ ET DE REPORTING

Infoblox utilise un modèle basé sur des jetons qui s'adapte à la manière dont vous défendez votre infrastructure et à l'endroit où vous le faites. Les jetons de sécurité permettent d'accéder à Threat Defense, SOC Insights, Dossier et à la surveillance des domaines similaires. Les jetons de reporting sont utilisés pour exporter les journaux DNS vers des SIEM, des SOAR ou des Data Lake pour une visibilité et une corrélation plus approfondies.

Ce système flexible élimine les niveaux de produits rigides et aligne les licences sur votre déploiement réel, que ce soit dans le cloud, sur site ou dans des environnements hybrides. Les jetons évoluent au fur et à mesure de la croissance de votre entreprise et peuvent être réaffectés entre les différentes fonctionnalités pour suivre l'évolution de vos priorités. Grâce à une visibilité centralisée via le portail des licences et à un modèle clair adapté à l'utilisation, vous pouvez plus facilement prévoir, budgétiser et démontrer le retour sur investissement de vos opérations de sécurité.

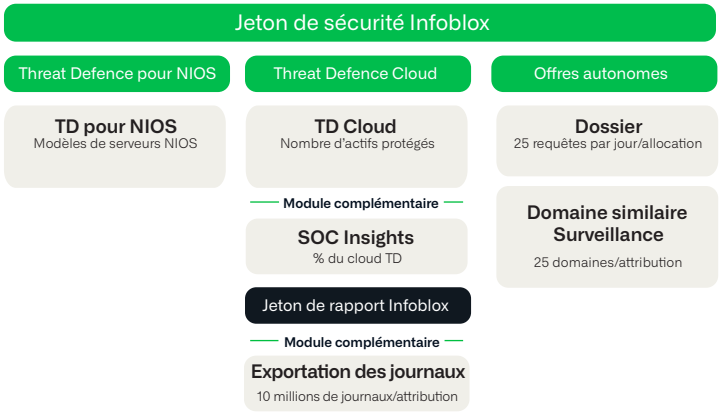

Figure 4. Structure de l'offre : sécurité et rapports

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 à un module SOC Insights.

- Aidez les analystes à se concentrer sur l'essentiel grâce à des analyses pilotées par l'IA, qui condensent des centaines de milliers d'alertes en quelques insights clés.
- Automatisez la journalisation, la threat intelligence et les autres tâches de collecte et de corrélation des données, afin que les analystes puissent lancer rapidement leurs investigations et interventions.
- Accélérez la réponse aux incidents grâce à la découverte des actifs et à l'intégration des inventaires, ce qui aide les analystes à identifier plus rapidement les appareils impactés.

EXPORTATION DE JOURNAUX DNS DE HAUTE VALEUR À GRANDE ÉCHELLE

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

- Filtrez et transférez uniquement les événements DNS de grande valeur afin de réduire les coûts d'ingestion SIEM et le bruit des alertes.
- Diffusez en temps réel des journaux DNS enrichis à l'aide du Cloud Data Connector d'Infoblox.
- Améliorez la détection et la réponse dans l'ensemble de 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 Indicateurs de compromission (IOC) et accélérer les enquêtes, sans avoir besoin de basculer entre différentes plateformes.

- Consolidez votre Threat Intelligence interne, celle proposée par Infoblox et par des tiers 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.

PROTÉGEZ VOTRE MARQUE CONTRE LA TROMPERIE 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 tromperie. 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 une validation humaine des incidents et à des rapports de synthèse.
- Coordonnez avec les fournisseurs d'accès Internet mondiaux, les hébergeurs et les organismes de réglementation pour un retrait rapide, souvent dans les 24 heures.
- Surveillez les menaces atténuées pendant 30 jours après leur suppression pour détecter et supprimer les tentatives de réactivation sans frais supplémentaires.
- Traitez plusieurs types de menaces, y compris le phishing, l'hébergement de malwares, les infrastructures de commande et contrôle, ainsi que le vol de données.

Pour en savoir plus sur la manière dont Infoblox Threat Defense sécurise vos données et votre infrastructure, veuillez visiter 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