

Infoblox Threat Defense™ Business Cloud

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

PROTÉGER AVANT L'IMPACT AVEC UNE SÉCURITÉ DNS FONDAMENTALE

La protection des infrastructures, des données et des utilisateurs est plus compliquée que jamais. Les modèles de sécurité traditionnels et réactifs ne suffisent plus. Les menaces d'aujourd'hui sont plus rapides, plus intelligentes et conçues pour contourner les défenses classiques.

- Les attaques alimentées par l'IA, comme les domaines similaires, le smishing, le contournement de l'authentification multi-facteurs (MFA) et le phishing ciblé, évoluent trop rapidement pour que les outils traditionnels puissent les détecter.
- Le périmètre a disparu. Désormais, les utilisateurs se connectent directement aux applications cloud depuis n'importe où, créant des lacunes que les outils traditionnels ne peuvent pas combler.
- Les sites distants et les succursales SD-WAN se connectent souvent directement à Internet, contournant ainsi les points d'inspection centralisés.
- L'IoT et les appareils non génèrent des angles morts que la sécurité des terminaux ne peut pas protéger seule.
- La plupart des outils traditionnels reposent sur la détection de malwares connus ou le filtrage de contenu, des approches réactives qui sont trop lentes face aux attaquants d'aujourd'hui.

Pour conserver une longueur d'avance, les entreprises ont besoin d'une **protection évolutive et préventive au niveau DNS**. Infoblox offre une sécurité DNS fondamentale capable d'identifier et de bloquer les menaces avant qu'elles n'atteignent les endpoints, les workloads cloud ou les succursales. Grâce à une visibilité inégalée, une intelligence prédictive et une intégration transparente à votre infrastructure de sécurité globale, Infoblox aide à réduire le bruit des alertes, à simplifier les opérations et à prévenir les attaques avant qu'elles ne causent des dommages.

SÉCURITÉ DNS PROTECTRICE À GRANDE ÉCHELLE

À mesure que les réseaux modernes se développent à travers les centres de données, le SD-WAN, les services cloud et les infrastructures IoT, maintenir une couverture de sécurité cohérente devient plus complexe, mais plus crucial que jamais.

Infoblox Threat Defense™ Business Cloud offre une sécurité DNS évolutive et native du cloud, renforçant votre posture de sécurité de bout en bout en protégeant votre environnement actuel et vos initiatives numériques en évolution, sans ajouter de charges opérationnelles. Qu'il s'agisse de protéger le DNS sur site, d'étendre la visibilité aux succursales distribuées ou de soutenir les utilisateurs à distance, Infoblox assure l'application au niveau DNS là où vous en avez besoin.

FONCTIONNALITÉS CLÉS

- Prévenez les menaces modernes en bloquant les ransomwares, le phishing, les exploits et les malwares grâce à la Threat Intelligence en temps réel.
- Empêchez l'exfiltration de données grâce à l'analyse et à l'apprentissage automatique, en arrêtant le DNS tunneling, les algorithmes de génération de domaine (DGA), DNSMessenger et l'activité à flux rapide.
- Protégez tous les appareils, qu'ils soient sur ou hors réseau, gérés ou non (BYOD, IoT, OT), au niveau DNS.
- Appliquez les politiques de contenu grâce au filtrage web et aux contrôles d'accès basés sur les utilisateurs.
- Protégez votre marque grâce à [la surveillance des domaines similaires](#), qui détecte et permet la suppression des usurpations de domaines malveillants.
- Accélérez les investigations jusqu'à trois fois grâce à une télémétrie DNS enrichie et au contexte des menaces.
- Améliorez la visibilité en corrélant l'activité DNS avec les métadonnées des actifs de gestion des adresses IP (IPAM) pour une réponse aux incidents plus rapide et plus précise.
- Priorisez et répondez plus rapidement aux menaces essentielles grâce à [SOC Insights](#) et au support d'enquêtes pilotées par l'IA.
- Intégrez l'ensemble de votre écosystème en partageant automatiquement la Threat Intelligence et les journaux avec le SIEM, le SOAR, les pare-feux nouvelle génération (NGFW), l'IPS, les endpoints et d'autres outils de sécurité.

Grâce à la threat intelligence en temps réel, à la visibilité unifiée et à l'intégration avec les outils SOAR et SIEM, les équipes de sécurité peuvent détecter, hiérarchiser et réagir plus rapidement. Cela réduit le temps de résolution des incidents, améliore les performances de votre infrastructure de sécurité existante et diminue le coût global de la protection contre les menaces au sein de l'entreprise.

Fourni depuis le cloud, Infoblox Threat Defense Business Cloud s'adapte facilement à l'évolution des besoins des clients, sans ajouter de complexité opérationnelle. À mesure que les besoins augmentent pour les utilisateurs, les sites et les charges de travail, la sécurité s'étend automatiquement avec vous.

L'AVANTAGE SAAS D'INFOBLOX

Infoblox Threat Defense Business Cloud est une solution logicielle en tant que service (SaaS) qui apporte des fonctionnalités de sécurité de nouvelle génération à votre infrastructure locale existante. Basée dans le cloud et facilement évolutive, la solution permet :

- Une amélioration immédiate de la posture de sécurité de l'entreprise
- Une couverture de sécurité simple pour tous les appareils, partout
- Une charge informatique minimale

« Aujourd'hui, trop de ransomwares, logiciels espions (spyware) et logiciels publicitaires (adware) circulent via des liens ouverts par les utilisateurs d'Internet. La solution de sécurité cloud d'Infoblox aide à bloquer les redirections vers des sites malveillants, à prévenir l'infection des machines et à protéger les utilisateurs. »

Administrateur système senior et
ingénieur réseau,
City University of Seattle

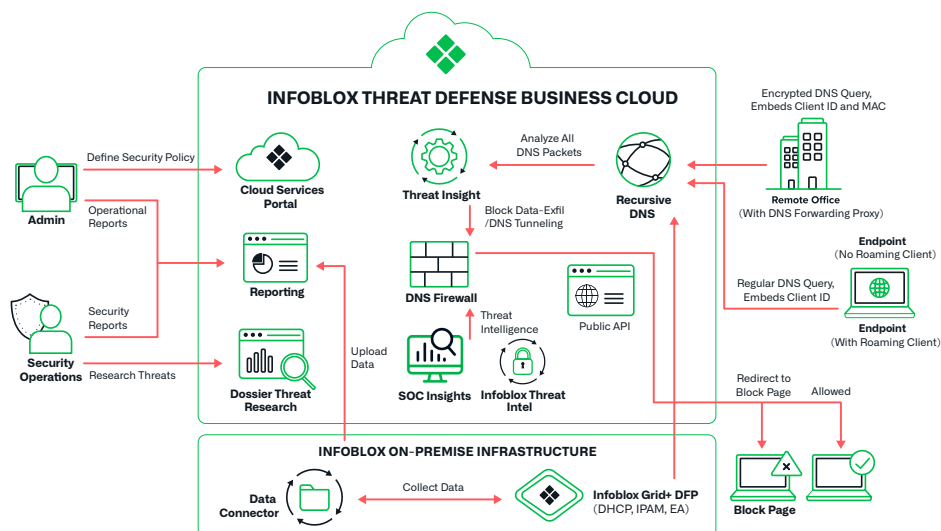


Figure 1. Scénario de workflow : Infoblox Threat Defense Business Cloud

PROXY DE TRANSMISSION DNS

Pour les environnements où l'installation d'un agent sur les endpoints n'est pas possible — comme les dispositifs IoT, les imprimantes ou les systèmes hérités — Infoblox fournit un proxy de transmission DNS (DFP) pour maintenir la visibilité au niveau des appareils et l'application des politiques.

Cette appliance virtuelle légère intègre l'adresse IP d'origine du client dans les requêtes DNS avant de les transférer vers le cloud Infoblox. Cela garantit une attribution précise des sources, une protection contre les menaces et une application cohérente, sans nécessiter d'agents locaux.

Intégré à Infoblox NIOS 8.3 et versions ultérieures, le proxy permet aux clients existants d'activer la sécurité DNS basée sur le cloud sans infrastructure supplémentaire sur site ni déploiement de logiciels.

L'agent Infoblox Endpoint fournit une protection sécurisée au niveau DNS pour les appareils mobiles, garantissant ainsi visibilité et contrôle même lorsque les utilisateurs travaillent hors réseau.

Cet agent léger peut être installé sur des ordinateurs portables ou des postes de travail pour assurer la visibilité et l'application des politiques, même lorsque les appareils sont hors du réseau d'entreprise.

- Redirige les requêtes DNS vers le cloud Infoblox pour inspection et application des politiques.
- Chiffre le trafic et étiquette chaque requête avec l'identité de l'appareil et le contexte utilisateur.
- Permet l'attribution au niveau utilisateur pour les enquêtes et rapports sur les incidents.
- Passe automatiquement en mode contournement lorsque l'appareil se trouve sur un réseau d'entreprise protégé.

Associé au proxy de transmission DNS, l'Endpoint Agent offre aux entreprises une couverture complète pour tous les utilisateurs, appareils et environnements, sans perte de visibilité ni de protection.

FONCTIONNALITÉS INTÉGRÉES

Disponibilité

Infoblox Threat Defense Business Cloud garantit une disponibilité DNS de 99,999 % (hors maintenance), grâce à une distribution Anycast mondiale, des sauvegardes quotidiennes et une surveillance 24 heures sur 24 et 7 jours sur 7.

Sécurité

Toutes les requêtes DNS et les données stockées sont chiffrées en transit et au repos. Les contrôles d'accès permettent des restrictions basées sur le rôle, l'adresse IP et la localisation.

Confidentialité

Infoblox suit les meilleures pratiques de sécurité, en appliquant des patchs réguliers, des analyses de code et des tests de pénétration. Les données des clients sont logiquement séparées, authentifiées via des clés API uniques et ne sont jamais partagées avec des tiers.

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



Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et par des innovateurs émergents. Nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

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

+1.408.986.4000
www.infoblox.com/fr