NOTE DE SYNTHÈSE

INFOBLOX ET GOOGLE CLOUD : PERFORMANCE ET PROTECTION POUR LES ENVIRONNEMENTS CLOUD HYBRIDES

SOLUTION DDI (DNS, DHCP ET GESTION DES ADRESSES IP) SUR GOOGLE CLOUD

Google Cloud permet aux entreprises de gagner en agilité et de réduire leurs coûts grâce à une approche cloud hybride, combinant infrastructures locales et services de cloud public comme Google Cloud. Cependant, la gestion des services réseau critiques tels que le DNS, le DHCP et la gestion des adresses IP (DDI) dans cet environnement peut entraîner des inefficacités et une visibilité limitée sur les réseaux virtuels, les VLAN, les adresses IP et les enregistrements DNS, ainsi que des défis de sécurité accrus en raison de la nature distribuée de l'infrastructure. Sans une solution de niveau entreprise pour automatiser et centraliser la gestion du DDI, des retards de service, des incohérences et des failles de sécurité peuvent survenir. Les solutions Infoblox pour Google Cloud peuvent aider à résoudre ces défis du cloud hybride.

Les solutions Infoblox DDI et Infoblox Threat Defense™ (Figure 1) permettent aux entreprises de gérer et de sécuriser centralement les services réseau essentiels et de se protéger contre les menaces dans les environnements cloud hybrides, tout en préservant les investissements, en optimisant le retour sur investissement et en s'adaptant aux exigences futures de l'entreprise.

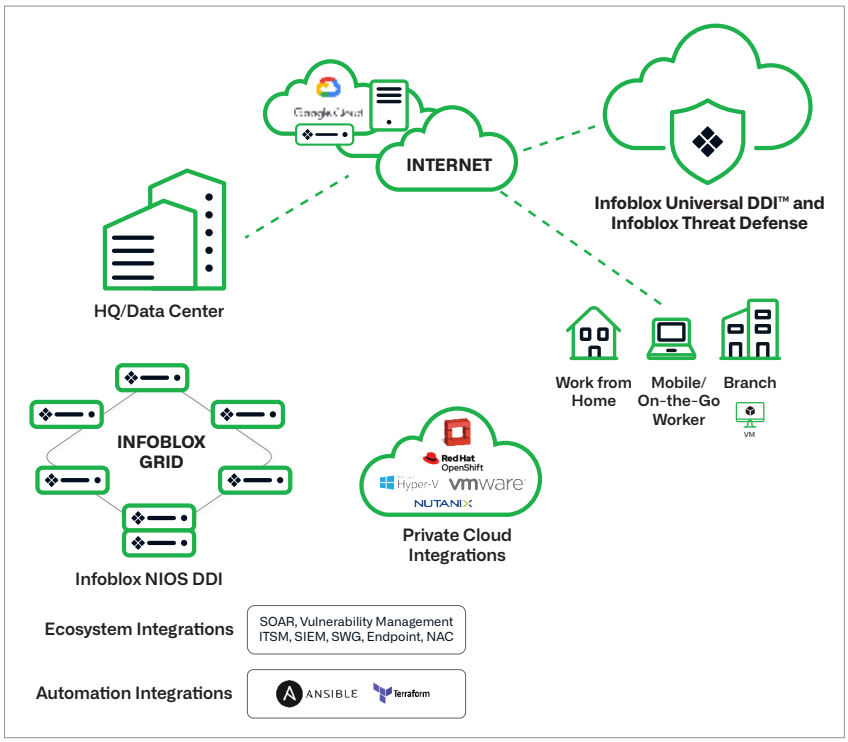

Figure 1. Solutions Infoblox DDI et Infoblox Threat Defense

LES AVANTAGES

Bénéficiez d'une gestion DNS et d'adresses IP (IPAM) de pointe pour Google Cloud

Automatisez la création, la suppression et la modification des enregistrements DNS pour les workloads Google Cloud.

Améliorez la découverte et la visibilité

Éliminez les zones d'ombre grâce à la découverte automatisée et à la visibilité unifiée et approfondie des réseaux virtuels et des machines sur Google Cloud.

Assurez la cohérence

Infoblox IPAM garantit la cohérence entre réseaux hybrides, sur site et Google Cloud.

Sécurité optimale

Threat Defense offre une sécurité DNS robuste pour détecter, bloquer et neutraliser les menaces.

Infoblox DDI simplifie l'IPAM

Infoblox étend ses services DDI à Google Cloud, offrant une meilleure visibilité, automatisation et contrôle dans les environnements multi-cloud privés, hybrides et publics. Grâce à Infoblox IPAM, vous pouvez gérer plusieurs systèmes IPAM (sur site et dans le cloud public) depuis un point de contrôle central, assurant ainsi une efficacité accrue, une meilleure coordination et des politiques de conformité optimisées.

Infoblox DDI (Figure 2) a récemment intégré **les plages internes de Google Cloud** pour vous aider à gérer efficacement les adresses IP de vos réseaux sur site et Google Cloud à grande échelle grâce à l'automatisation.

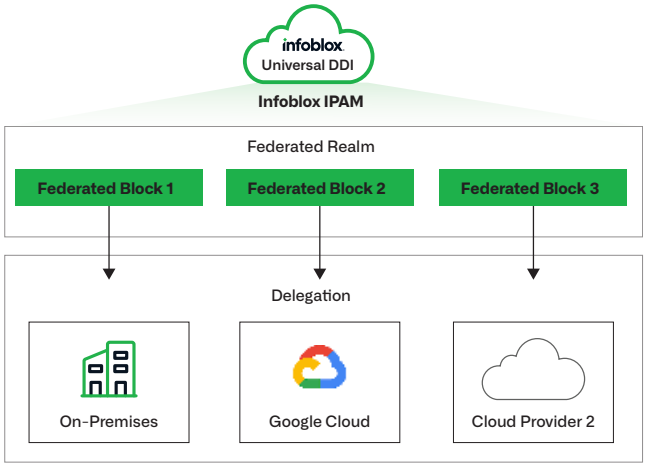

Figure 2. Universal DDI et Infoblox IPAM

Infoblox Threat Defense renforce la sécurité réseau et stoppe les cybermenaces

En plus d'une visibilité, d'une automatisation et d'une gestion constantes des services réseau essentiels, les solutions Infoblox offrent une sécurité DNS de pointe pour les charges de travail exécutées sur site et dans le cloud. Threat Defense (Figure 3) fournit des services DNS hybrides de protection pour sécuriser les réseaux, les appareils et les utilisateurs contre les cybermenaces, que ce soit sur site, hors site, ainsi que dans les sites distants et les bureaux à domicile.

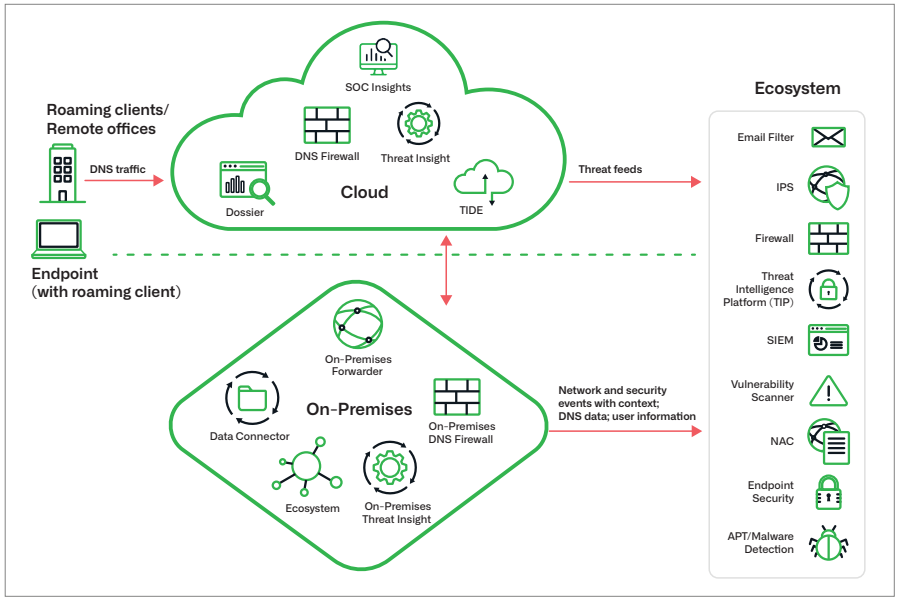

Figure 3. Services DNS hybrides de protection

Détection et réponse aux menaces DNS

Threat Defense analyse les requêtes DNS pour détecter et bloquer les communications de commande et de contrôle de malwares, les domaines suspects, l'exfiltration de données via DNS, le phishing, les ransomwares et les menaces avancées telles que les algorithmes de génération de domaines (DGA) et les domaines ressemblants. La solution s'appuie sur Infoblox Threat Intel, une intelligence sur les menaces unique, centrée sur le DNS, qui analyse en profondeur le trafic DNS du réseau client pour identifier les acteurs malveillants et bloquer leurs domaines avant qu'ils ne lancent des attaques.

Intégrations à l'écosystème

Threat Defense facilite également une réponse plus rapide aux menaces grâce à l'utilisation d'API et d'intégrations natives prêtes à l'emploi avec des outils de l'écosystème de sécurité, notamment les SIEM, SOAR, ITSM, scanners de vulnérabilités, NAC, et solutions de sécurité des endpoints. La solution améliore considérablement la posture de sécurité des environnements hybrides. En s'appuyant sur les données DDI, Threat Defense utilise un contexte réseau précieux (comme la localisation du segment et les charges de travail compromises) pour identifier rapidement la menace et lancer les actions de remédiation avant toute propagation latérale.

infoblox.

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

Version : 20250512v2