

NOTE DE SYNTHÈSE

INFOBLOX ET GOOGLE CLOUD PLATFORM : PERFORMANCES ET PROTECTION POUR LES ENVIRONNEMENTS CLOUD HYBRIDES

SOLUTION DNS, DHCP ET IPAM (DDI) SUR GCP

Google Cloud permet aux entreprises de gagner en agilité et de réduire leurs coûts grâce à une approche hybride, combinant infrastructures locales et services cloud comme Google Cloud Platform. Cependant, la gestion des services réseau essentiels, DNS, DHCP et gestion des adresses IP (DDI), dans cet environnement peut entraîner des pertes d'efficacité et une visibilité limitée sur les réseaux virtuels, les VLAN, les adresses IP et les enregistrements DNS, ainsi qu'une augmentation des enjeux de sécurité en raison de la nature distribuée de l'infrastructure. Sans une solution de qualité professionnelle pour automatiser et centraliser la gestion des DDI, des délais de service, des incohérences et des failles de sécurité peuvent apparaître. Les solutions Infoblox pour Google Cloud Platform peuvent aider à résoudre ces défis du cloud hybride.

Infoblox DDI et BloxOne® 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 protégeant les investissements, en optimisant le retour sur investissement et en s'adaptant aux exigences futures de l'entreprise.

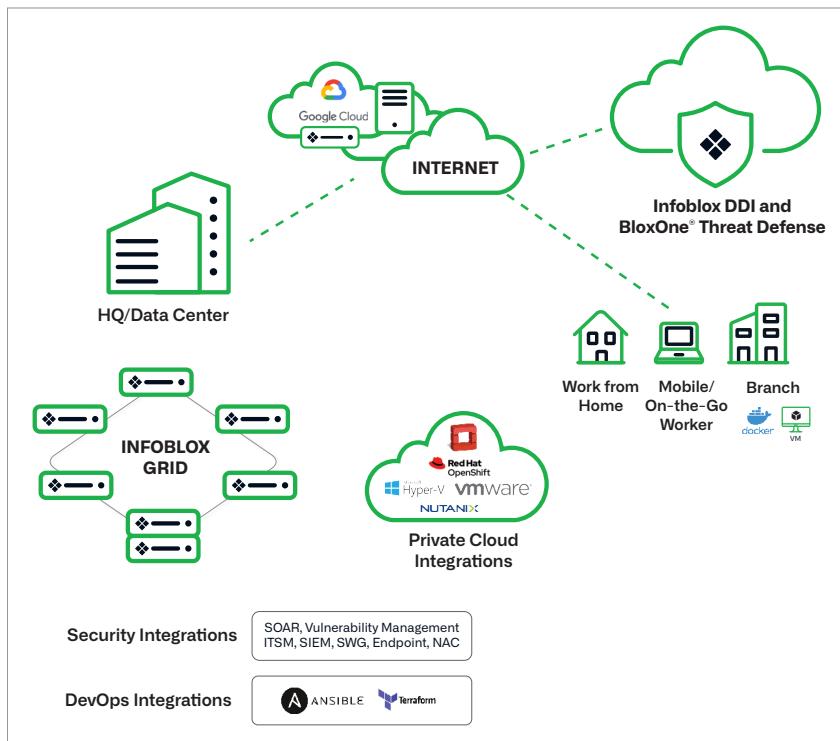


Figure 1 : solutions Infoblox DDI et BloxOne® Threat Defense

LES AVANTAGES

Bénéficiez d'une gestion de pointe des adresses IP et DNS pour GCP

Automatissez l'ajout, la suppression et les modifications des enregistrements DNS pour les charges de travail GCP.

Améliorez la découverte et la visibilité

Supprimez les failles grâce à la découverte automatisée et à la visibilité unifiée et légale des réseaux virtuels et des machines virtuelles sur GCP.

Assurez la cohérence

Infoblox IPAM garantit la cohérence sur les réseaux hybrides, sur site et GCP.

Sécurité optimale

BloxOne Threat Defense offre une sécurité fiable basée sur le DNS pour détecter, bloquer et résoudre les menaces de sécurité.

Infoblox DDI simplifie la gestion des adresses IP (IPAM)

Infoblox a étendu sa plateforme d'automatisation cloud à Google Cloud Platform, améliorant ainsi la visibilité, l'automatisation et le contrôle dans les environnements multi-clouds 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 optimisées de conformité.

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

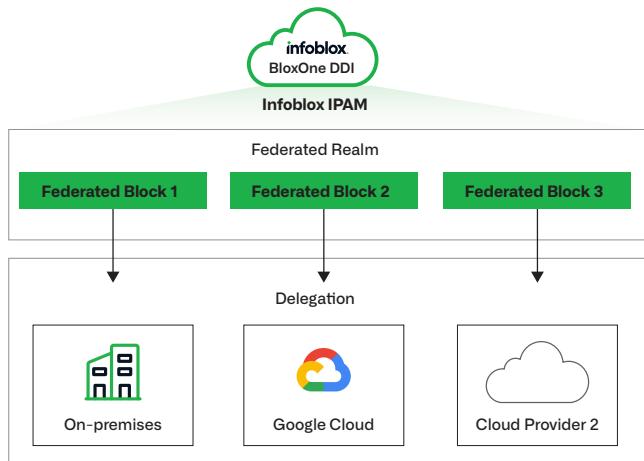
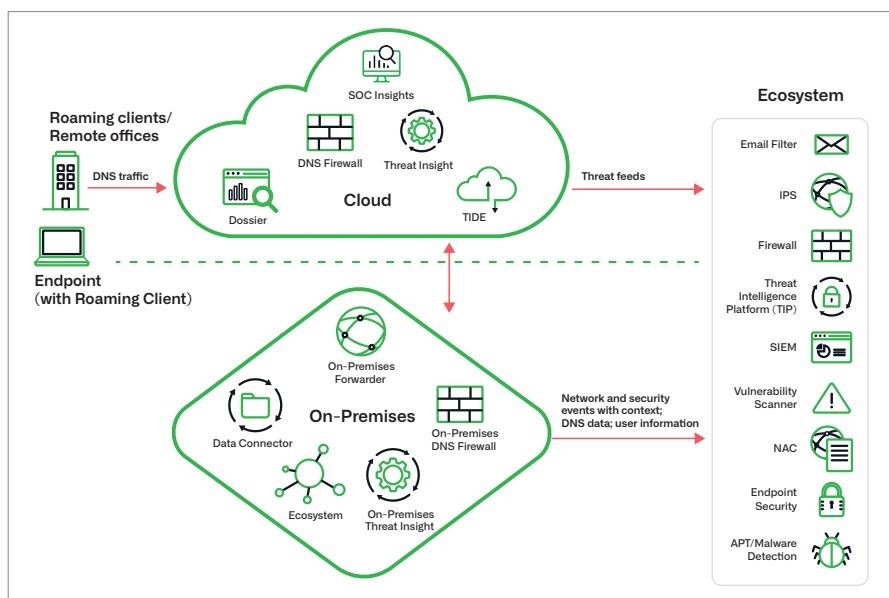


Figure 2 : Infoblox DDI et Infoblox IPAM

BloxOne® Threat Defense améliore la sécurité du réseau et arrête les cybermenaces

En plus de la visibilité, de l'automatisation et de la gestion cohérentes des services réseau essentiels, les solutions Infoblox aident à fournir une sécurité DNS de pointe pour les charges de travail exécutées sur site et dans le cloud. Infoblox BloxOne® Threat Defense (Figure 3) fournit des services DNS hybrides de protection pour sécuriser les réseaux, les appareils et les utilisateurs contre les cybermenaces sur et hors site, y compris les sites distants et les bureaux à domicile.



Détection et réponse aux menaces DNS

BloxOne® Threat Defense analyse les requêtes DNS pour détecter et bloquer les communications C&C de malware, les domaines suspects, l'exfiltration de données basée sur le DNS, le phishing, les ransomwares et les menaces avancées telles que les algorithmes de génération de domaines (DGA) et les domaines similaires. La solution s'appuie sur Infoblox Threat Intel, une solution unique centrée sur le DNS, et l'inspection du trafic DNS du réseau client pour identifier les cybercriminels et bloquer leurs domaines avant qu'ils n'attaquent.

Intégrations de l'écosystème

BloxOne® Threat Defense contribue également à accélérer la réponse aux menaces en utilisant des API et des

intégrations natives prêtes à l'emploi avec des outils de l'écosystème de sécurité, notamment SIEM, SOAR, ITSM, des scanners de vulnérabilité, le contrôle d'accès au réseau et la sécurité des endpoints. La solution améliore considérablement la posture de sécurité pour les environnements hybrides. En s'appuyant sur les données DDI, BloxOne Threat Defense utilise un contexte réseau précieux, tel que la partie du réseau et les charges de travail compromises, afin d'identifier et de lancer rapidement une action de résolution des problèmes avant que la menace ne se propage latéralement.



Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et les 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