

# ÉCOSYSTÈME INFOBLOX

Éliminez les silos, automatisez les flux de travail et renforcez votre sécurité

L'écosystème Infoblox unifie votre écosystème de réseau et de sécurité, permettant un échange de données bidirectionnel fluide. Il simplifie les opérations en automatisant les flux de travail, améliore la détection des menaces et renforce les capacités de réponse dans les environnements sur site, hybrides et multi-cloud.

En automatisant les services réseau essentiels et en partageant une visibilité précoce des menaces, des adresses IP fiables et des données réseau contextuelles (comme l'attribution des utilisateurs et des appareils) avec vos outils de réseau et de sécurité existants, les intégrations éliminent les silos, améliorent votre efficacité opérationnelle et renforcent l'ensemble de votre pile de sécurité informatique.

## ARCHITECTURE DE L'ÉCOSYSTÈME INFOBLOX

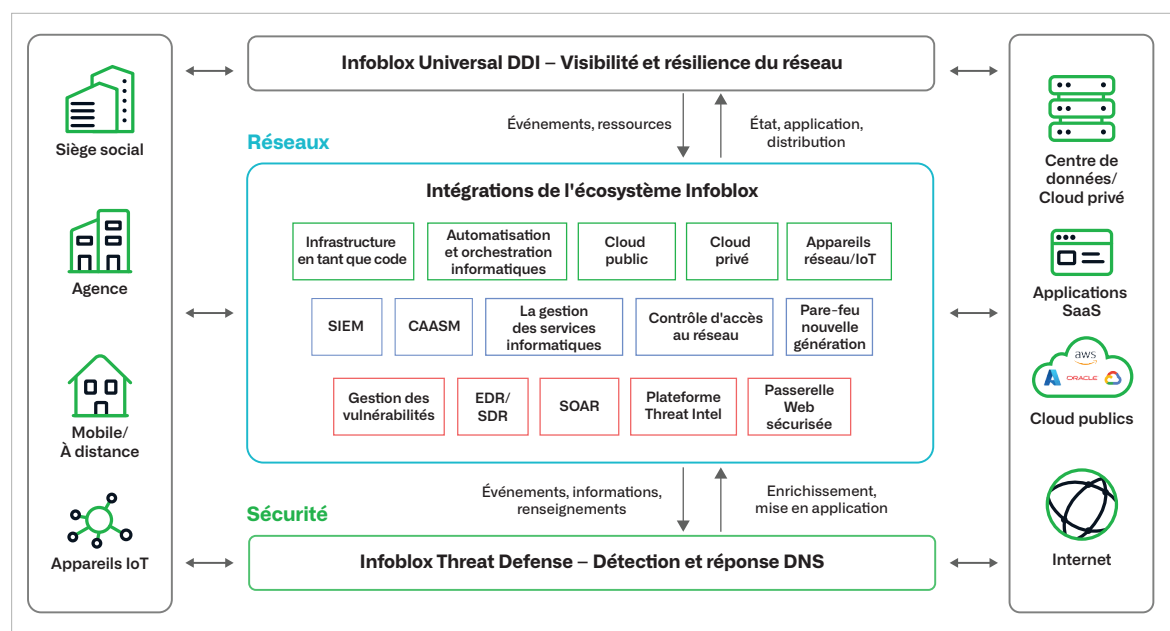


Figure 1 : Architecture de l'écosystème Infoblox

Que vous ayez recours à des clouds publics/privés, à la gestion des services informatiques, à la gestion des informations et des événements de sécurité (SIEM)/à l'orchestration, l'automatisation et la réponse aux incidents de sécurité (SOAR) ou d'autres outils de sécurité, Infoblox garantit une intégration fluide pour renforcer vos environnements hybrides et multi-cloud. Parcourez notre vaste gamme d'**intégrations certifiées prédéfinies** sur le [Portail de l'écosystème Infoblox](#). Elle sont conçues pour fonctionner sans accroc et elles débloquent tout le potentiel de vos solutions réseau et sécurité avec Infoblox.

## Les avantages de l'écosystème Infoblox :

- **Réduction du risque de failles de sécurité** : Lorsque vous éliminez les silos et améliorez la collaboration entre les outils de réseau et de sécurité, il devient plus difficile pour les pirates informatiques d'exploiter des vulnérabilités.
- **Amélioration de l'efficacité opérationnelle** : L'automatisation des flux de travail et la réduction des tâches manuelles permettent aux équipes informatiques de réaliser des gains de temps considérables et de gagner en efficacité.
- **Meilleur retour sur investissement** : En tirant le meilleur parti de vos outils de réseau et de sécurité existants, l'écosystème Infoblox vous aide à maximiser votre investissement informatique.

Technologie de l'écosystème	Aperçu de l'intégration	Les avantages
La gestion des informations et des événements de sécurité (SIEM)	<ul style="list-style-type: none"> <li>• Infoblox envoie des événements de BloxOne Threat Defense SOC Insights, dont des informations sur les adresses IP, les appareils infectés et des requêtes et réponses DNS suspectes au SIEM.</li> <li>• L'équipe SecOps peut ensuite utiliser ces informations sur les incidents pour effectuer une analyse et prendre les mesures appropriées.</li> </ul>	<ul style="list-style-type: none"> <li>• Réduit la surcharge d'alertes en fournissant des informations SOC corrélées directement à votre SIEM</li> <li>• Offre une vue d'ensemble de l'activité des appareils, quelle que soit l'origine des journaux.</li> <li>• Enrichit le contexte pour mieux hiérarchiser les événements de sécurité</li> <li>• Améliore l'efficacité opérationnelle des équipes SecOps et informatiques</li> </ul>
L'orchestration, automatisation et réponse aux incidents de sécurité (SOAR)	<ul style="list-style-type: none"> <li>• La solution SOAR reçoit des événements liés à BloxOne Threat Defense SOC Insights, dont des informations sur l'adresse IP, les périphériques réseau et les événements malveillants, ainsi que des informations d'Infoblox.</li> <li>• SOAR utilise ces informations pour arrêter, débloquer et contrôler le domaine et vérifier les informations sur l'adresse IP, l'hôte, le réseau et le domaine dans la gestion des adresses IP (IPAM). Infoblox enrichit automatiquement l'IPAM avec des données provenant d'outils et d'événements de sécurité.</li> </ul>	<ul style="list-style-type: none"> <li>• Fournit un contexte complet des appareils et des utilisateurs pour mettre en évidence les risques et enrichir les playbooks SOAR</li> <li>• Automatise et accélère la réponse grâce à l'ensemble des API de threat intelligence</li> <li>• Améliore les processus de sécurité en s'intégrant à d'autres systèmes via SOAR</li> </ul>
Gestion des vulnérabilités (VM)	<ul style="list-style-type: none"> <li>• Infoblox envoie des informations sur les nouveaux appareils réseau et les événements malveillants à la gestion des vulnérabilités.</li> <li>• La gestion des vulnérabilités utilise ces informations pour déclencher automatiquement des analyses sélectives, permettant une découverte complète des ressources, une remédiation plus rapide des problèmes et une meilleure conformité.</li> </ul>	<ul style="list-style-type: none"> <li>• Offre une visibilité quasi en temps réel des nouveaux appareils rejoignant le réseau</li> <li>• Automatise et accélère la réponse aux modifications du réseau et aux événements malveillants</li> <li>• Facilite l'analyse sélective basée sur les ressources</li> </ul>

Technologie de l'écosystème	Aperçu de l'intégration	Les avantages
Plateforme Threat Intelligence (TIP)	<ul style="list-style-type: none"> <li>• Infoblox Threat Intelligence Data Exchange (TIDE) envoie automatiquement des informations sur les noms d'hôtes, les adresses IP et les URL malveillants à la plateforme TIP.</li> <li>• La TIP permet de bloquer et de surveiller un plus grand nombre de menaces.</li> </ul>	<ul style="list-style-type: none"> <li>• Comble les lacunes en matière de protection, notamment en ce qui concerne les domaines à haut risque, Zero Day DNS™, les domaines similaires, etc.</li> <li>• Assure une application cohérente des politiques sur tous les points de contrôle</li> <li>• Renforce la posture de sécurité globale</li> </ul>
Le contrôle d'accès réseau (NAC)	<ul style="list-style-type: none"> <li>• Infoblox fournit des informations sur les adresses IP, les appareils réseau et les événements de sécurité DNS.</li> <li>• Les solutions NAC peuvent utiliser ces informations pour obtenir un contexte permettant de mieux hiérarchiser les menaces et de prendre des mesures plus immédiates (comme retirer l'appareil du réseau) afin de réduire le délai de neutralisation.</li> </ul>	<ul style="list-style-type: none"> <li>• Améliore la visibilité de l'infrastructure du réseau, des utilisateurs et des appareils</li> <li>• Fournit un contexte vital pour la hiérarchisation des menaces</li> <li>• Permet d'agir en temps utile, par exemple en mettant en quarantaine les appareils compromis</li> </ul>
Gestion des services informatiques (ITSM) et opérations de sécurité	<ul style="list-style-type: none"> <li>• Infoblox crée automatiquement un ticket informatique lorsque de nouveaux appareils rejoignent le réseau ou que des événements malveillants sont détectés, avec des informations détaillées sur l'appareil et l'utilisateur.</li> <li>• Infoblox fournit également ces informations aux outils de communication informatique. Les administrateurs de réseau et de sécurité bénéficient d'une vue consolidée de toutes les informations sur les appareils et les événements découverts par Infoblox.</li> </ul>	<ul style="list-style-type: none"> <li>• Offre des vues de tableau de bord instantanées sur les appareils et endpoints rejoignant et quittant le réseau</li> <li>• Permet l'identification proactive des problèmes de réseau afin d'accélérer la réponse aux changements de réseau et aux événements de sécurité</li> </ul>
Cloud public	<ul style="list-style-type: none"> <li>• Infoblox fournit une gestion centralisée et simplifiée des services réseau essentiels, du DNS, du DHCP et de la gestion des adresses IP (DDI) dans les environnements publics et multi-cloud.</li> <li>• Intégrations avec les principaux fournisseurs de cloud, notamment Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).</li> </ul>	<ul style="list-style-type: none"> <li>• Augmente l'agilité grâce à l'automatisation des enregistrements DNS et des adresses IP à l'aide d'intégrations prédéfinies</li> <li>• Fournit une vue holistique des ressources sur les réseaux publics/multi-cloud et rationalise la conformité.</li> <li>• Permet d'évoluer de manière élastique et d'étendre les charges de travail aux clouds publics</li> </ul>

Technologie de l'écosystème	Aperçu de l'intégration	Les avantages
Cloud privé	<ul style="list-style-type: none"><li>• Infoblox DDI pour le cloud privé et la virtualisation simplifie et automatise les services de gestion des DNS, DHCP et adresses IP sur des charges de travail multi-plateformes, vous permettant ainsi de maximiser votre stratégie de cloud privé.</li></ul>	<ul style="list-style-type: none"><li>• Stimule la productivité et l'efficacité sur le cloud privé et les flux de travail virtuels</li><li>• Fournit des informations sur les instances virtuelles et rationalise la conformité et l'audit</li><li>• Assure la cohérence essentielle à la sécurité, à l'efficacité et à la fiabilité du réseau</li></ul>
L'infrastructure en tant que code (IaC)	<ul style="list-style-type: none"><li>• Le plug-in Infoblox pour les plateformes IaC telles que Hashicorp Terraform étend les services IPAM et DNS aux clouds privés virtuels (VPC), aux réseaux virtuels (VNET) et aux machines virtuelles (VM) sur les plateformes cloud.</li></ul>	<ul style="list-style-type: none"><li>• Optimise la visibilité, l'automatisation et le contrôle du réseau grâce aux intégrations IPAM et DNS incluses</li><li>• Stimule l'efficacité en déchargeant les développeurs d'applications de la responsabilité et de l'affectation du réseau</li><li>• Identifie en permanence les ressources virtuelles sur plusieurs plateformes afin de rationaliser le suivi et l'audit.</li></ul>
Automatisation et orchestration informatiques	<ul style="list-style-type: none"><li>• Le plug-in Infoblox pour les technologies d'automatisation et d'orchestration telles qu'Ansible, OpenStack, Terraform, VMware, etc., simplifie et rationalise la distribution et la récupération des adresses IP pour les nouvelles machines virtuelles, met à jour les enregistrements DNS et génère des adresses IP en quelques secondes au lieu de plusieurs heures, voire jours.</li></ul>	<ul style="list-style-type: none"><li>• Permet une automatisation complète et améliore l'efficacité opérationnelle informatique</li><li>• Fournit une visibilité approfondie de l'infrastructure physique et virtuelle, et accélère la résolution des problèmes</li><li>• Réduit les coûts et les délais liés à la complexité des déploiements de serveurs virtuels</li></ul>
Découverte des appareils réseau/IoT	<ul style="list-style-type: none"><li>• Infoblox automatise la découverte des appareils réseau et IoT dans les applications tierces, synchronise les données collectées pour fournir une base de données fiable et une vue unifiée des ressources</li></ul>	<ul style="list-style-type: none"><li>• Offre une visibilité sans précédent sur des infrastructures réseau complexes</li><li>• Augmente l'agilité en supprimant les silos informatiques</li><li>• Réduit les risques en identifiant plus rapidement les appareils malveillants</li></ul>

Pour en savoir plus, rendez-vous sur le [portail de l'écosystème Infoblox](#).



Infoblox unifie le réseau et la sécurité pour offrir des performances et une protection sans égales. Reconnu par les entreprises listées au classement Fortune 100 et les innovateurs émergents, nous offrons une visibilité et un contrôle en temps réel sur les personnes et les appareils se connectant au réseau d'une organisation afin d'accélérer son fonctionnement et d'arrêter les menaces plus tôt.

**Siège social**  
2390 Mission College Boulevard,  
Ste. 501 Santa Clara, CA 95054  
  
+1.408.986.4000  
[www.infoblox.com](http://www.infoblox.com)