

NOTE DE SYNTHÈSE

CONSTRUIRE UNE INFRASTRUCTURE AGILE ET RÉILIENTE

Dans le contexte commercial actuel, caractérisé par un rythme soutenu et une forte concurrence, l'agilité et l'innovation sont les moteurs de la réussite d'une entreprise. À mesure que la technologie évolue, les réseaux modernes doivent s'adapter, suivre le rythme de l'innovation en tirant parti des dernières avancées, permettre le déploiement efficace de nouvelles applications et de nouveaux services, et offrir la flexibilité nécessaire pour répondre aux demandes changeantes du marché.



LE RYTHME DE LA MODERNISATION EST IMPLACABLE

D'ici 2026, au moins 50 % des applications sur site seront modernisées pour s'intégrer aux outils de la plateforme de gestion SaaS (SMP), contre 20 % en 2021, selon un rapport de Gartner. Avec la numérisation, les réseaux deviennent plus dynamiques et évoluent en permanence. Divers facteurs, y compris le télétravail, l'expansion multi-cloud, les nouvelles exigences en cybersécurité et le besoin de nouvelles compétences, contribuent à l'accélération de la modernisation.

LIMITES DES SERVICES RÉSEAU ESSENTIELS HÉRITÉS

L'infrastructure réseau inclut de nombreux composants : pare-feu, routeurs, commutateurs, dispositifs Wi-Fi, serveurs de noms de domaine, serveurs DHCP, et bien d'autres encore. La plupart des éléments des infrastructures stratégiques sont déjà en cours de mise à niveau vers des versions matérielles ou logicielles modernes. Qu'en est-il des serveurs de noms de domaine et des serveurs DHCP ? Vos services réseau fondamentaux sont-ils toujours obsolètes ? S'appuyer sur des services réseau hérités, des logiciels gratuits, des solutions maison ou des systèmes disparates constitue un obstacle majeur à votre transition numérique.

- **Ces systèmes sont *disjoints*** : la gestion manuelle est coûteuse et présente un risque élevé de temps d'arrêt et de pannes.
- **Les systèmes hérités sont *lents*** : les réseaux doivent être agiles pour adopter de nouvelles idées et technologies dans le cadre d'initiatives stratégiques de numérisation ou de fusions et acquisitions (M&A).
- **Les systèmes hérités sont *exposés*** : les failles de sécurité et le manque de connaissance contextuelle entraînent une remédiation inefficace et tardive des menaces.

Le DNS et le DHCP sont essentiels pour tous les réseaux, et si vous utilisez encore des services natifs, votre réseau est exposé à des pannes massives.

PRINCIPAUX MOTEURS DE LA MODERNISATION : LA VOIE À SUIVRE

Les entreprises modernisent leur réseau pour faire face aux défis des réglementations croissantes, aux contraintes de ressources, aux menaces en constante évolution et aux manques de compétences dans le domaine de la sécurité. Elles doivent constamment réduire les temps d'arrêt, gérer les frais généraux et minimiser les failles de sécurité afin d'assurer un temps de fonctionnement de 100 %, d'adopter de nouvelles idées et d'améliorer la pile de sécurité existante. Cela nécessite de repenser les approches des opérations réseau critiques, y compris la gestion du DNS, du DHCP et des adresses IP (collectivement « DDI »). Voici les principaux moteurs pour moderniser votre réseau.



RATIONALISER LES OPÉRATIONS : REMPLACER LES LOGICIELS GRATUITS PAR DES OUTILS CONÇUS SPÉCIFIQUEMENT

Gratuit n'est pas vraiment gratuit. Même si les dépenses initiales peuvent sembler moindres, les coûts opérationnels que vous engagerez en utilisant des outils DDI gratuits ou à faible coût dépasseront les avantages. Les solutions gratuites comme Microsoft ou les outils open source ne peuvent pas évoluer pour soutenir la croissance en raison des limitations du système et du manque de fonctionnalités avancées pour assurer une plus grande disponibilité, la découverte de machines virtuelles inutilisées, les validations basées sur des politiques, etc. Les infrastructures Microsoft sont sujettes aux pannes et aux temps d'arrêt, soit en raison de mises à jour constantes des correctifs, soit parce qu'elles doivent être migrées vers Azure AD. La gestion manuelle des sites distribués accroît l'inefficacité et augmente les coûts généraux.

La meilleure approche consiste à tirer parti des **outils conçus spécifiquement** pour simplifier et rationaliser les opérations essentielles. Ces outils sont conçus pour la mondialisation et vous permettent de réduire les tâches opérationnelles en s'étendant de manière transparente à diverses infrastructures et à des sites à distance. Ils simplifient la gestion, optimisent la maintenance et réduisent le temps grâce à l'automatisation, à la découverte et à la visibilité centralisée du réseau. Ils offrent des mises à niveau sans interruption et réduisent les temps d'arrêt en assurant une plus grande disponibilité à grande échelle.



ACCÉLÉRER LES INNOVATIONS : UTILISEZ UN SEUL OUTIL CENTRALISÉ AU LIEU DE SYSTÈMES DISPARATES

La plupart des entreprises utilisent deux à quatre solutions DNS, ce qui complique la gestion des services essentiels et rend plus difficile la résolution rapide des problèmes. Les silos organisationnels et informationnels causent souvent des retards et des erreurs. Les différentes conventions de dénomination et modèles opérationnels des divers fournisseurs de cloud entraînent des erreurs de configuration et des interruptions de service. La visibilité fragmentée à travers les réseaux augmente le temps nécessaire pour la résolution des problèmes et l'audit.

Les entreprises doivent trouver une solution efficace et efficiente pour accélérer les innovations et permettre des initiatives commerciales telles que l'expansion multi-cloud, les fusions et acquisitions, etc. Investir dans **un outil centralisé** vous permettra d'atteindre ces objectifs grâce à l'automatisation, à une convention de nommage DNS unique et à la visibilité sur les réseaux sur site et cloud. Au lieu d'utiliser un mélange de systèmes disparates, vous pouvez vous adapter plus rapidement aux besoins de l'entreprise et réduire les inefficacités grâce à un outil centralisé. Il offre un contrôle des politiques et une cohérence, une résolution plus rapide des problèmes et une meilleure collaboration, évite les mauvaises configurations et les erreurs, et réduit les risques d'audit et de conformité ainsi que les coûts opérationnels.



PROTÉGER L'INTÉGRITÉ DE LA MARQUE : UTILISER LE DNS POUR DÉTECTER LES MENACES TÔT

Les domaines en constante évolution que constituent les menaces informatiques, telles que les malwares, les ransomwares, les domaines similaires, l'exfiltration de données et le phishing, représentent des risques considérables pour l'identité des marques et la protection des données. Il existe une faille de sécurité importante, car les solutions existantes sur le marché négligent le DNS et ne parviennent pas à prévenir les attaques. Au cours de l'année écoulée seulement, les pirates ont utilisé près de 42 000 domaines usurpés dans une attaque de phishing massive. En outre, les systèmes cloisonnés et disparates, le manque de compétences, la gestion manuelle et le manque de conscience contextuelle entraînent des inefficacités dans les opérations de sécurité (SecOps) et des retards dans les temps de réponse.

La détection précoce des menaces réduit les risques et comble les failles de sécurité. L'utilisation de **la recherche de menaces basée sur le DNS** permet de détecter et de bloquer les menaces plus rapidement, car la plupart des cyberattaques s'appuient sur le DNS. L'utilisation du DNS comme première ligne de défense protège contre l'exfiltration de données, les algorithmes de génération de domaines et les imposteurs, et sécurise tous les appareils IoT/OT. Elle améliore l'efficacité des opérations de sécurité en réduisant le temps d'investigation, en automatisant la résolution des problèmes et en évaluant de manière proactive les risques de vulnérabilité.

SOLUTIONS INFOBLOX POUR UNE INFRASTRUCTURE AGILE ET RÉSILIENTE

Visibilité, automatisation et contrôle

Infoblox offre aux entreprises une visibilité, une automatisation et un contrôle inégalés sur les personnes et les appareils qui se connectent à leur réseau. Infoblox réduit considérablement les temps d'arrêt coûteux en supprimant la maintenance encombrante et obligatoire, en automatisant les tâches opérationnelles à forte intensité de main-d'œuvre, et en réduisant le fardeau associé à la gestion de l'inventaire des actifs réseau. Les solutions Infoblox sont conçues dans un souci de sécurité, réduisant les fausses alertes grâce à une meilleure connaissance du contexte et améliorant l'efficacité. Infoblox fournit :

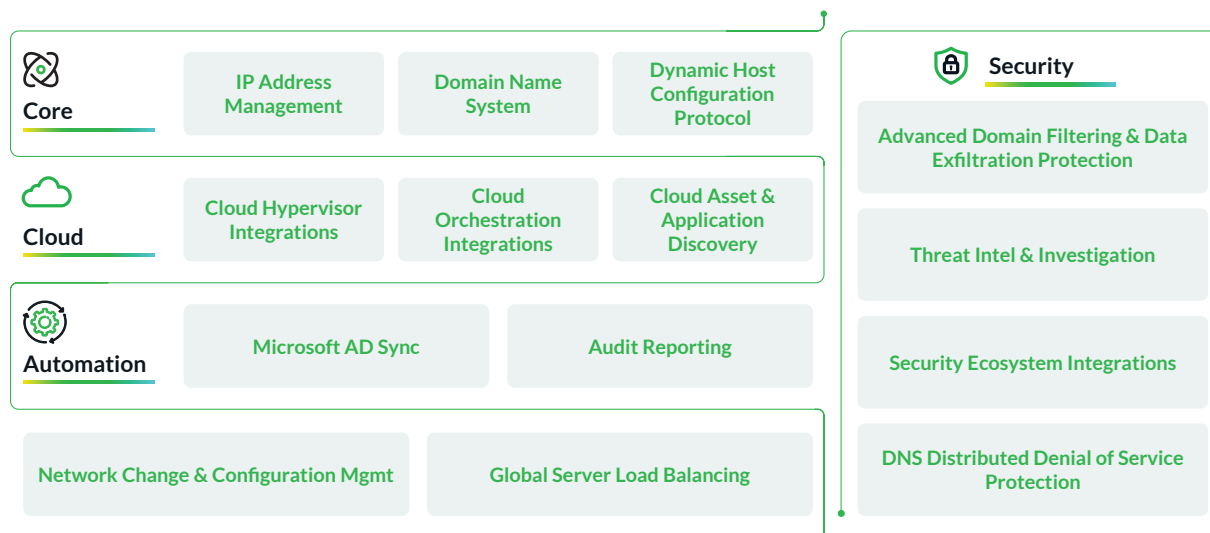


Figure 1 : solutions Infoblox

CONCLUSION

La modernisation stimule la transformation numérique. Choisir la solution adaptée à votre réseau garantit une modernisation continue. Les approches héritées de la gestion des services réseau stratégiques entravent votre capacité à innover rapidement, à vous adapter à l'évolution des besoins de l'entreprise et à rester compétitif. Tirez parti de la visibilité, de l'automatisation et du contrôle qu'Infoblox offre pour moderniser votre réseau à la vitesse nécessaire et adaptée à la croissance de votre entreprise.



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