FICHE TECHNIQUE

Infoblox pour les équipes sécurité des télécoms

Renforcez l'efficacité de la sécurité, la résilience opérationnelle et la performance des SecOps

LE DÉFI

Aujourd'hui, les réseaux des fournisseurs de services de communication (FSC) évoluent vers des clouds télécoms s'étendant aux environnements privés, publics et hybrides. Cette évolution élargit les domaines opérationnels au RAN, aux réseaux câblés et centraux, aux clouds privés et publics, ainsi qu'aux sites edge multi-accès. Avec le déplacement du calcul et du stockage vers la périphérie pour permettre de nouveaux types de traitement et de distribution des services sur des milliers de sites, le risque de menaces de sécurité augmente considérablement, qu'elles proviennent d'applications tierces ou d'attaquants externes. Les opérateurs stockent de grandes quantités de données personnelles et sont responsables de la stabilité de leurs services de communication. Le déploiement généralisé de dispositifs hors du centre de données expose également un nombre croissant de points d'accès et crée une surface de menace massive que les cybercriminels peuvent exploiter. Une violation de données ou une défaillance de service résultant d'une cyberattaque peut entraîner de graves préjudices financiers et de réputation ou avoir un impact sur les clients, un coup dur pour toute entreprise dans un marché hautement concurrentiel.

Avec le déploiement de ressources toujours plus nombreuses à la périphérie du réseau, les équipes IT et sécurité des opérateurs doivent gérer un nombre nettement plus élevé de pods, de machines virtuelles, parfois par centaines, et potentiellement des milliers de conteneurs, dans des environnements physiques, virtuels et cloud. Les appareils non corrigés peuvent devenir des points de vulnérabilité. Bien que la protection des endpoints avec des capacités de détection et de réponse soit indispensable, les équipes de sécurité déjà surchargées doivent impérativement reconnaître les signes d'une attaque, quelles que soient les circonstances, dans un réseau en constante évolution et en pleine croissance. Les fournisseurs de services de communications exigent des solutions de cybersécurité éprouvées qui augmentent leur visibilité pour identifier les menaces modernes, limiter les enquêtes et accroître l'efficacité des réponses aux incidents.

LA SOLUTION

Les solutions Infoblox pour les fournisseurs permettent les connexions IP cruciales entre les abonnés et leur monde numérique. Nous unissons la gestion DNS, DHCP et des adresses IP (DDI) afin d'automatiser la visibilité, l'évolutivité et la gestion du réseau. Nos solutions réduisent le temps de réponse aux incidents de deux tiers en permettant à tous les composants majeurs de votre pile de sécurité, y compris les systèmes de sécurité, d'orchestration, d'automatisation et de réponse (SOAR), de répondre aux événements de sécurité plus tôt, avant qu'ils ne causent des dommages. Nous aidons également les fournisseurs à minimiser les interruptions d'activité causées par les DDoS et autres risques et attaques basés sur le DNS.

FONCTIONNALITÉS CLÉS

Renforcez la protection de la sécurité
Détectez et bloquez les exploits, le phishing, les ransomwares et autres malwares modernes qui échappent aux autres solutions.

Augmentez la visibilité
Bénéficiez d'une visibilité précise et d'un contexte réseau riche en intégrant les métadonnées des actifs de gestion des adresses IP pour une compréhension et une corrélation optimales des événements.

Accélérez la réponse aux incidents
Réduisez le délai de correction en corrélant automatiquement les événements, le réseau et la threat intelligence provenant de dizaines de sources afin d'accélérer les enquêtes jusqu'à deux tiers.

Améliorez le ROI en sécurité
Optimisez vos efforts grâce à des défenses renforcées et une plus grande efficacité des opérations de sécurité. Maximisez la valeur de vos plateformes SIEM, SOAR et autres outils de sécurité.

Allégez la charge des équipes de sécurité
Bénéficiez d'informations enrichies sur les événements et les menaces, ainsi que d'analyses IA/ML appliquées au DNS, pour une protection évolutive contre les malwares modernes et les menaces DNS.

Infoblox réduit le coût total de la défense contre les menaces en allégeant le fardeau des défenses extérieures. Nos solutions permettent aux équipes de sécurité de tirer un meilleur parti de vos solutions de sécurité tierces grâce au partage bidirectionnel en temps réel des informations sur les événements de sécurité et à l'automatisation qui réduit les coûts associés aux efforts manuels et aux erreurs humaines. Les analystes de sécurité peuvent obtenir une vue unique sur la Threat Intelligence associée à un événement et réduire le temps d'analyse des menaces jusqu'à deux tiers.

Minimisez les interruptions de réseau
Maintenez l'intégrité du DNS et prévenez les attaques DDoS DNS externes et internes qui peuvent mettre votre réseau hors ligne.

LES AVANTAGES CLÉS

Arrêtez les menaces que les autres protections ne détectent pas

De meilleures informations sur les menaces rendent chaque outil de sécurité plus efficace. BloxOne® Threat Defense recueille, rassemble et agrège des informations sur les menaces provenant d'Infoblox, de vos autres outils commerciaux et de sources gouvernementales tierces. L'Infoblox Cyber Intelligence Unit (CIU) améliore la précision tout en minimisant les faux positifs et vous permet de tout personnaliser en fonction de vos besoins. Un « super-flux » normalisé peut ensuite être partagé dans l'ensemble de la pile de sécurité, ce qui renforce l'efficacité de chaque défense.

Bloquez les malwares et l'exfiltration de données

BloxOne Threat Defense opère au niveau du DNS pour détecter les menaces que les autres solutions ne voient pas et arrêter les attaques plus tôt dans le cycle de vie de la menace. Bloquez l'accès aux sites malveillants, les communications par commande et contrôle (C&C), le vol de données basé sur le DNS et d'autres activités malveillantes en utilisant la Threat Intelligence et l'IA/ML

Minimisez les interruptions d'activité

Le DNS est fondamental pour toute organisation car il fournit une connectivité réseau critique. Si votre DNS est défaillant, votre entreprise l'est aussi. Les attaques DDoS réussies peuvent coûter à une organisation des centaines de milliers de dollars de perte de revenus par mois. Infoblox Advanced DNS Protection (ADP) vous protège efficacement contre le plus grand nombre d'attaques DNS DDoS et préserve le temps de fonctionnement de votre organisation.

Accélérez les investigations et les remédiations

Les analystes doivent avoir accès à des informations fiables sur les menaces et à d'autres données contextuelles autour d'un événement afin d'accélérer les réponses. Avec Dossier™, dans le cadre de BloxOne Threat Defense, les analystes obtiennent une vue unique sur les renseignements sur les menaces associées à un événement. L'accès rapide à des informations spécifiques à un événement peut réduire de deux tiers le temps d'investigation des menaces.

Améliorez SIEM, SOAR et plus

Armées d'une multitude d'outils de défense renforcée, les équipes de cybersécurité peuvent être débordées par la nécessité de gérer manuellement des dizaines d'outils de sécurité et de répondre à des centaines, voire des milliers d'alertes chaque jour. L'échange d'écosystème Infoblox offre un ensemble d'intégrations interconnectées qui permettent aux équipes de sécurité d'éliminer les silos, d'optimiser leurs solutions de SOAR et SIEM et d'améliorer le retour sur investissement de leur écosystème de cybersécurité.

Allégez les charges SecOps grâce à l'automatisation

BloxOne Threat Defense offre de nombreuses fonctionnalités qui vous permettent d'exploiter plus facilement la threat intelligence, les informations sur les événements et d'autres données. L'automatisation élimine les charges de gestion et rend les processus d'investigation et de réponse de SecOps plus efficaces. Réduisez la charge pesant sur les dispositifs de sécurité périmétrique sollicités, tels que les pare-feux, les IPS et les proxys Web, en utilisant vos serveurs DNS existants comme première ligne de défense.

Simplifiez et optimisez la gestion des modifications et de la configuration du réseau

De nombreux problèmes réseau résultent de changements, d'erreurs liées aux modifications manuelles des appareils et de configurations incorrectes, qui engendrent par la suite des dysfonctionnements et affaiblissent les politiques de sécurité essentielles ainsi que la protection du réseau. Infoblox NetMRI est une solution de gestion des modifications et des configurations réseau qui automatise les flux de travail courants tels que le provisionnement des appareils et les opérations de sécurité, garantissant ainsi une conformité renforcée et une réponse plus rapide en cas d'incident.

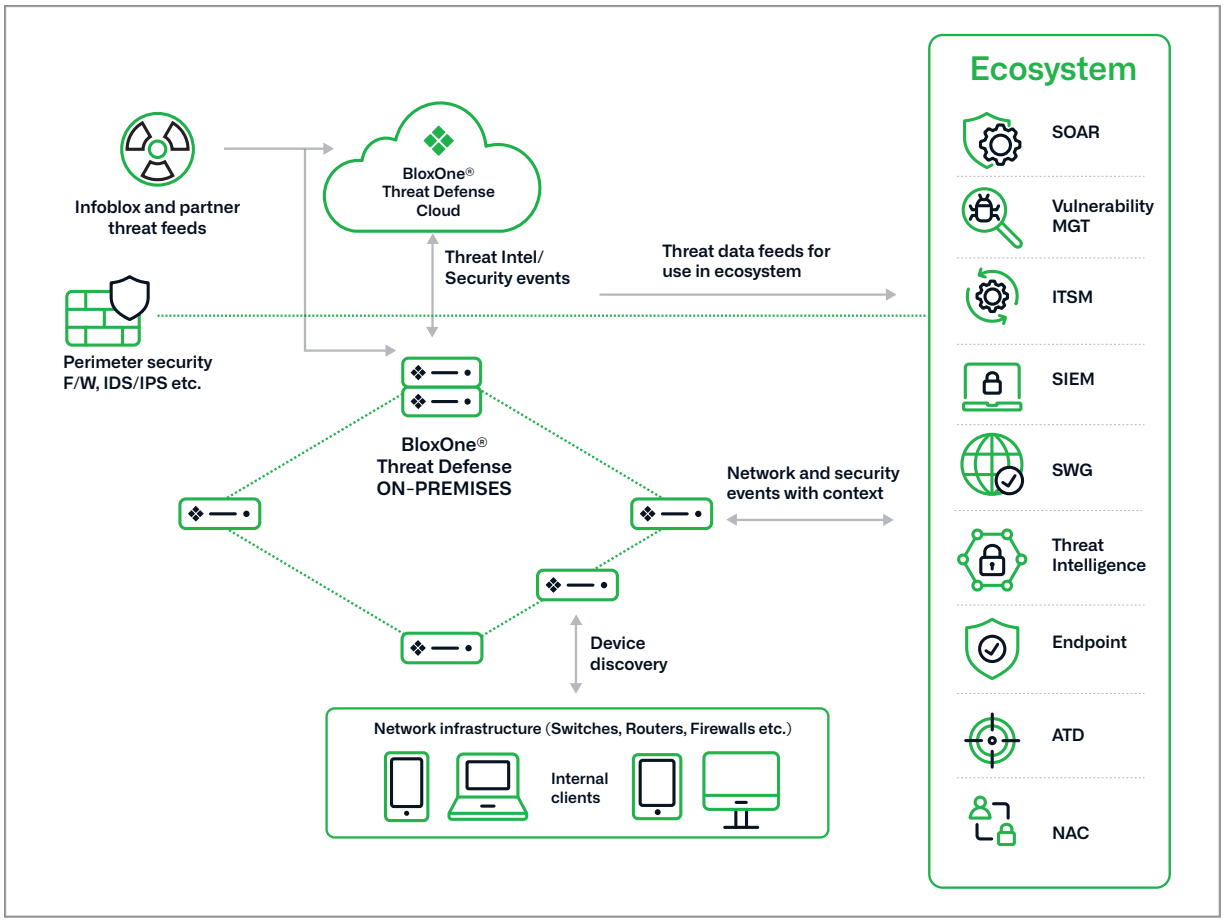

Figure 1 : Infoblox renforce et optimise les réseaux des fournisseurs de services de communication

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

Version : 20240521v1