

Gigamon Hawk Cloud Visibility and Analytics Fabric

Surveillance et sécurité unifiées du réseau pour toutes les infrastructures

À mesure que les opérations réseau passent de déploiements d'appareils physiques monolithiques à des hôtes virtuels privés administrés, et que les développeurs d'applications passent des implémentations autonomes sur site au cloud public, être en mesure de gérer et de sécuriser de manière suffisante les réseaux ainsi que les applications s'avère de plus en plus difficile. Tout comme les opérateurs de réseaux physiques l'ont appris dans les années 1990 et 2000, s'appuyer uniquement sur les fichiers de logs et d'autres données provenant des fonctionnalités et des applications réseau elles-mêmes n'est pas fiable et requiert un développement constant à mesure que celles-ci changent ou sont mises à niveau. C'est ici que Gigamon Hawk entre en jeu.



La première véritable matrice de visibilité réseau pour les clouds hybrides physiques, privés et publics.
(Voir la Figure 1)

CARACTÉRISTIQUES PRINCIPALES

- Acquisition de trafic depuis n'importe quelle machine virtuelle, tout conteneur et toute infrastructure réseau physique
- Intelligence centralisée pour l'agrégation, la duplication, le tagging, le filtrage et la distribution du trafic vers les outils de surveillance et de sécurité
- Orchestration unifiée via des approches DevOps et la gestion de la matrice depuis une interface unique
- API RESTful pour l'intégration avec des outils et des infrastructures cloud

BÉNÉFICES PRINCIPAUX

- Visibilité complète du trafic réseau à travers l'ensemble de votre cloud hybride et de vos environnements matériels monolithiques
- Réduction de la complexité et des coûts, et amélioration de la performance de votre solution de surveillance et de sécurité sans avoir à sacrifier la couverture offerte
- Réduction des temps d'arrêt des applications
- Découverte de nouvelles charges de travail, acheminement approprié du trafic et ajustement du niveau de visibilité : le tout sans intervention manuelle

Pour des opérations cloud réussies, tous les réseaux doivent être couverts

Face au rythme toujours croissant de la transformation numérique, les opérations réseau et sécurité sont confrontées à des enjeux importants. Comment pouvez-vous, par exemple, maintenir des opérations sans interruption et assurer la sécurité de vos réseaux, services et applications dans une configuration hybride d'applications hébergées dans le cloud public et sur site.

Qu'il s'agisse de charges de travail dans le cloud public, dans un datacenter en cloud privé administré ou dans un datacenter physique, l'exploitation, la sécurité et la conformité continue des données et des applications réseau dépendent des équipes informatiques qui se doivent d'assurer que tout est déployé de manière sécurisée et fonctionne comme prévu. Afin de pouvoir identifier et de corriger automatiquement et de manière proactive les limitations de sécurité et de performance, vous devez disposer d'une visibilité précise et complète sur l'ensemble des environnements réseau.

DES RÉFLEXIONS INDISPENSABLES

Les architectes informatiques, cloud et de sécurité doivent répondre aux questions suivantes lors de la planification de toute migration ou extension réseau :

- + Comment puis-je m'assurer que tout le monde dans l'entreprise utilise le réseau et les applications en toute sécurité ?
- + Comment puis-je migrer des applications vers le cloud public tout en répondant aux besoins de contrôle de la conformité et de la sécurité ?
- + Si des failles de sécurité zero-day sont exploitées dans des logiciels non corrigés, quels sont les mécanismes dont je dispose pour pouvoir les détecter ?
- + Comment puis-je détecter et traiter des anomalies de sécurité ou du réseau lors du déploiement de nouvelles applications ou de la mise à niveau d'applications existantes ?
- + Comment puis-je obtenir une vue consolidée de l'ensemble des infrastructures par le biais de mes outils de surveillance et de sécurité ?
- + Existe-t-il des méthodes efficaces pour réduire le coût du trafic de réacheminement (backhauling) lorsque les outils de surveillance dans le cloud sont sur site plutôt que partie d'un ensemble d'outils dans le cloud ?
- + Comment puis-je surmonter les limitations du trafic mirroring et peering dans le cloud public, notamment en considérant les frais élevés de transmission de données ?

Ne pas tenir compte de ces éléments ralentit la migration des applications et des services vers les clouds privés et publics et vous rend vulnérable face à des failles de sécurité potentielles.

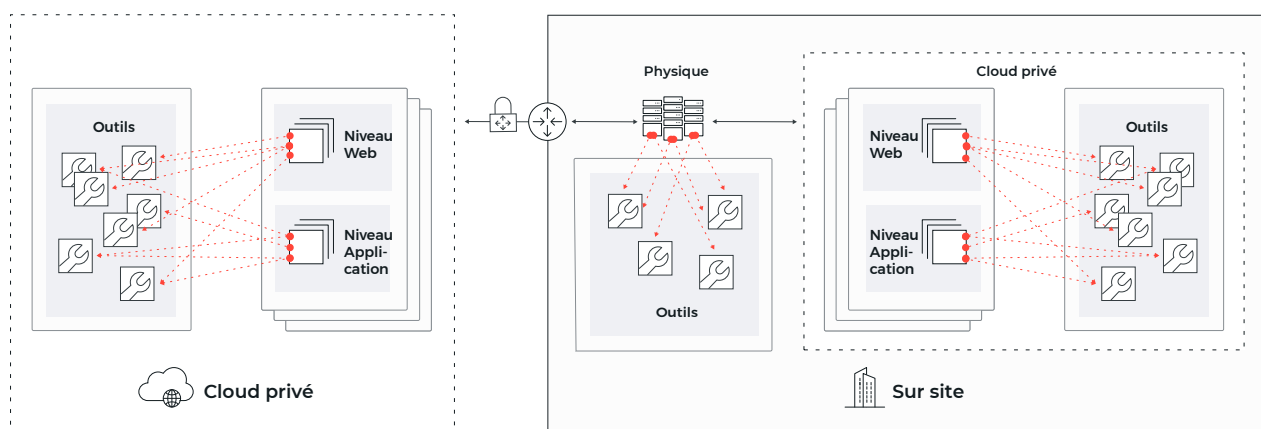


Figure 1. Un réseau hybride d'entreprise sans Gigamon Hawk.

La solution

Gigamon Hawk offre des capacités intelligentes de collecte de paquets et de flux, via un modèle de gestion simple, afin d'améliorer la sécurité, l'efficacité opérationnelle et l'évolutivité des infrastructures réseaux hybrides. Gigamon Hawk permet aux équipes NetOps et InfoSec de renforcer la visibilité pour la surveillance et la sécurité du réseau et de tirer le meilleur parti de leurs outils nouveaux et existants, les outils physiques existants pouvant même être utilisés pour le cloud privé sur site.

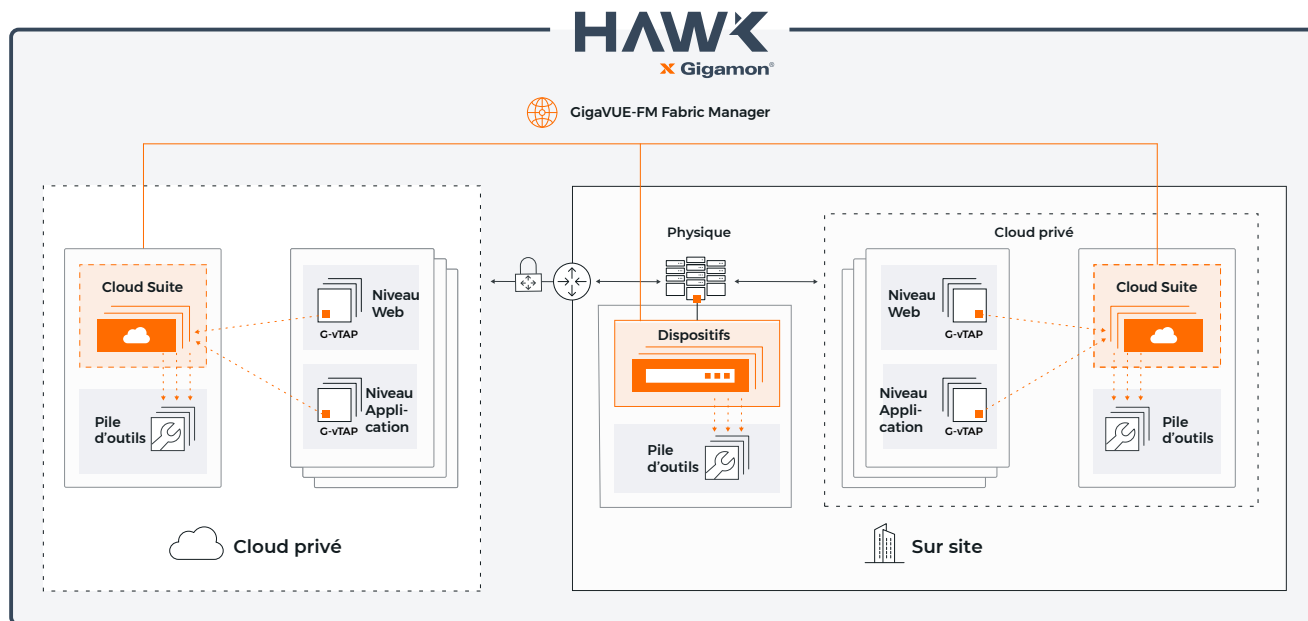


Figure 2 : Un réseau hybride d'entreprise avec Gigamon Hawk.

La solution comprend :

- + GigaVUE® Cloud Suite, avec des équipements de visibilité GigaVUE V Series et G-VTAP, afin de fournir des capacités de collecte, de traitement et de transmission du trafic au sein des infrastructures virtuelles et des conteneurs
- + Équipements physiques GigaVUE, avec GigaVUE HC/TA Series et G-TAP, afin de fournir des fonctionnalités de collecte, de traitement et de transmission du trafic au sein de l'infrastructure physique
- + GigaVUE-FM afin de fournir une gestion unifiée à guichet unique de la matrice de visibilité et d'analyse à travers l'ensemble des infrastructures

INTELLIGENCE DU TRAFIC

Bénéfices principaux :

- + Supprimer la duplication des paquets issus des ports miroir/SPAN de switch réseau, de plusieurs points TAP ou de plusieurs sources de mirroring virtuel, pouvant réduire ainsi le trafic de surveillance de plus de 50 %
- + Supprimer ou découper des paquets ou flux, entraînant une réduction de 75 % ou plus du trafic transmis vers les outils
- + Gagner de la visibilité sur le trafic crypté SSL/TLS, ceci incluant les flux cryptés TLS 1.3
- + Respecter les directives de protection des données grâce au masquage des données
- + Supprimer l'encapsulation et le tagging non souhaités,
- + augmentant ainsi l'efficacité et la performance de vos outils
- + Mise en place de tunnel pour les sources de trafic virtuelles, interconnexion multi-sites et le transfert vers des outils virtuels

RENSEIGNEMENTS SUR LES ABONNÉS

Bénéfices principaux :

- + Filtrer, mettre sur liste blanche et/ou échantillonner de manière cohérente les sessions des plans de contrôle et d'utilisateur 3G, 4G et 5G en se concentrant uniquement sur le trafic pertinent
- + Équilibrer de manière cohérente les charges 3G, 4G et 5G sur plusieurs instances du même outil
- + Filtrer de manière cohérente, établir une liste blanche et/ou un échantillonnage des sessions de signalisation SIP et de données RTP en se concentrant uniquement sur le trafic pertinent
- + Équilibrer de manière cohérente les charges SIP et RTP sur plusieurs instances du même outil

INTELLIGENCE APPLICATIVE

Bénéfices principaux :

- + Ignorer ou se concentrer sur des applications spécifiques au sein du trafic utilisateur, ce qui renforce l'efficacité et la performance de votre surveillance et de votre sécurité
- + Générer des métadonnées complexes pour les applications afin d'alimenter des outils de surveillance et de sécurité (par exemple, les SIEM) qui ne reçoivent pas les paquets de données brutes.
- + Générer des enregistrements de données vidéo pour les outils d'analyse vidéo (par exemple, PVA de Nokia AVA), sans avoir besoin de sondes séparées

RENSEIGNEMENTS DE SÉCURITÉ

Bénéfices principaux :

Générer des métadonnées intelligentes sur les menaces pour l'outil de détection et de réponse réseau (NDR) Gigamon ThreatINSIGHT™.

Conclusion

Que les opérations de votre entreprise se déroulent principalement dans le cloud, sur site ou même dans un environnement hybride, Gigamon Hawk offre une visibilité intelligente du trafic réseau pour les applications et les services fonctionnant dans votre cloud hybride. La gestion unifiée simplifie le déploiement d'un niveau de visibilité global agrégeant le trafic et appliquant une intelligence avancée avant de transmettre le trafic sélectionné vers les outils de surveillance et de sécurité. Avec Gigamon Hawk, vous pouvez enfin obtenir des informations cohérentes sur l'ensemble de votre infrastructure à travers les clouds publics et l'environnement sur site.

Pour de plus amples informations sur Gigamon Hawk, visitez gigamon.com.