




Cas d'usage Allot  
**Espaces Nomades**  
Entreprise

Contactez MERISAC pour une étude de votre projet  
"See, Control, Secure" dans le Cloud/Datacenter :

[merisac@merisac.com](mailto:merisac@merisac.com)  
Bureau : 01 49 33 737 5  
Mobile : 06 60 12 64 51

**MERISAC** ▲  
INSTRUMENTS  
Intégrateur de Services WAN & Datacenter

Traduction française assurée par les sociétés

 translated.

▲ **MERISAC** ▲  
INSTRUMENTS  
Intégrateur de Services WAN & Datacenter

# INTRODUCTION

---

Ce document fournit une sélection de cas d'usage Allot pour les clients du secteur des Espaces Nomades (Convention center, Aéroports, Hôtels,...). Chaque cas d'utilisation décrit un problème spécifique rencontré par les entreprises de ce secteur et fournit une description détaillée des produits disponibles qui peuvent être utilisés pour apporter des solutions à ces réseaux d'entreprise.

Les solutions d'Allot vous permettent d'augmenter la productivité et de protéger vos activités ainsi que vos utilisateurs contre les ransomware, les Attaques par déni de service et les infections par bot. En fournissant une visibilité totale et un contrôle granulaire des applications, des utilisateurs et de l'utilisation du réseau, la gamme Secure Service Gateway (SSG) d'Allot vous permet de supprimer les applications suspectes de votre réseau, de contrôler le trafic de loisir et, plus important encore, d'assurer que votre réseau fonctionne conformément à vos priorités métiers. En outre, les solutions Allot diminuent le coût total de possession de votre investissement en sécurité. Allot tire parti de la technologie DPI et de l'approche analytique du Big data pour fournir une

*Allot est un fournisseur leader de solutions d'optimisation de services IP intelligentes qui aident les entreprises et les centres de données à gérer des réseaux plus efficaces pour mieux satisfaire leurs utilisateurs.*

vision claire et précise de l'utilisation du réseau. Armés de ces précieuses informations, les responsables informatiques peuvent contrôler dynamiquement la livraison des applications critiques pour se conformer aux SLA, protéger les actifs du réseau contre les attaques et accélérer le retour sur investissement (ROI) effectué sur leur infrastructure informatique.

Les solutions Allot sont déployées à travers le monde entier dans des centres de données et des réseaux d'entreprise opérant dans un large éventail de secteurs d'activité, notamment le commerce électronique, l'éducation, l'énergie, les services publics,

la finance, l'administration publique, les soins de santé, l'enseignement supérieur, l'hôtellerie, les médias et les télécommunications, les commerces de détail et les transports.

Les cas pratiques présentés dans cette brochure sont basés sur les principaux avantages qui peuvent être obtenus soit directement par une entreprise, soit par des services managés d'opérateurs. Chaque cas tire profit des capacités de sécurité et d'intelligence réseau liées au comportement des applications, des utilisateurs et des équipements, ainsi que du contrôle des entreprises pour :

- Comprendre comment les ressources réseau sont consommées avant de réinvestir dans l'infrastructure
- Définir des politiques de gestion du trafic en temps réel qui alignent les performances sur les priorités de l'entreprise et ajustent dynamiquement les flux de trafic IP lorsque les liaisons WAN sont en congestion
- Définir des politiques de gestion du trafic hiérarchiquement en fonction des niveaux de service individuels destinés à des profils utilisateur spécifiques
- Réduire la surface d'attaque de l'entreprise et augmenter la productivité en identifiant et en bloquant les applications à risque telles que les anonymiseurs et les applications P2P
- Contrôler l'utilisation des applications informatiques non autorisées telles que le stockage dans le Cloud et les réseaux sociaux
- Augmenter la disponibilité grâce à une protection DDoS en temps réel combinée à une gestion du trafic afin de supprimer automatiquement le trafic des attaques DDoS en quelques secondes, tout en maintenant une qualité d'expérience (QoE) maximale de tous les services réseau légitimes et critiques de l'entreprise
- Détecter et neutraliser les menaces web, le phishing, les ransomware, les botnets de quarantaine et les hôtes infectés par des logiciels malveillants

### Atouts majeurs

- Permet l'utilisation d'appareils personnels pour améliorer la productivité des salariés de l'entreprise
- Assure que les appareils personnels ne perturbent pas le réseau
- Renforce les mesures de sécurité du réseau

### Permet d'utiliser des dispositifs personnels à des fins professionnelles

- Tient compte des règles BYOD dans le cadre de la stratégie de gestion Wi-Fi
- Détecte automatiquement le trafic provenant d'appareils personnels
- Applique en temps réel les règles liées aux BYOD
- Examine les rapports d'utilisation du BYOD pour évaluer et affiner la politique

### Généré par Secure Service Gateway (SSG) d'Allot

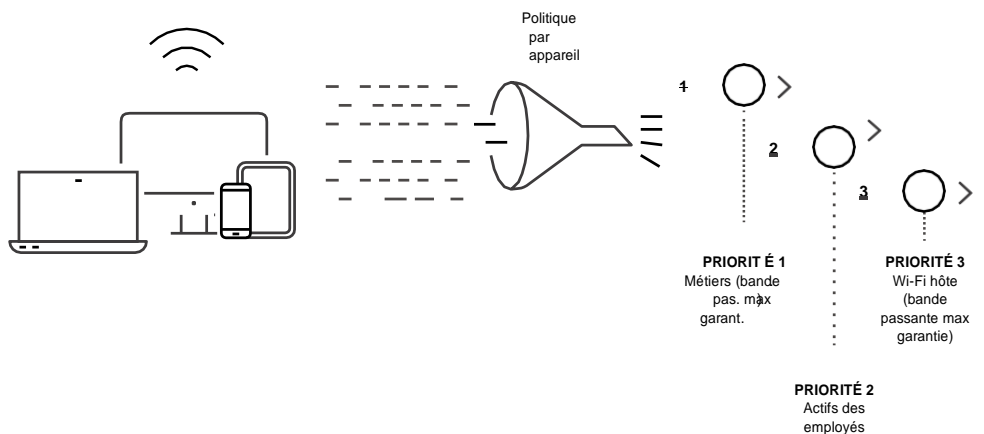
- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

## ESPACES NOMADES

# BRING YOUR OWN DEVICE (BYOD) ou APPORTEZ VOTRE APPAREIL PERSONNEL

Alors que de nombreux responsables informatiques considèrent le Bring-Your-Own-Device (BYOD) comme un casse-tête de plus qui ouvre la porte à des risques de sécurité sur le réseau, les utilisateurs y voient une formidable source de productivité et d'efficacité personnelles. Les entreprises doivent pouvoir appliquer les règles de contrôle sur des appareils personnels nomades une fois qu'ils sont sur le réseau. Par exemple, les règles liées au BYOD peuvent inclure une limitation en cas d'utilisation intensive, l'allocation de plus de bande passante aux appareils professionnels des salariés par rapport aux appareils des clients et la priorité aux applications métiers. La haute technologie d'inspection approfondie des paquets (Deep Packet Inspection, DPI) d'Allot fournit des signatures d'équipements de la même manière qu'elle fournit des signatures d'applicatives qui sont mises à jour régulièrement par le net. Cela garantit une identification rapide et précise des appareils qui n'appartiennent pas à l'entreprise et de leur trafic réseau.

### BYOD

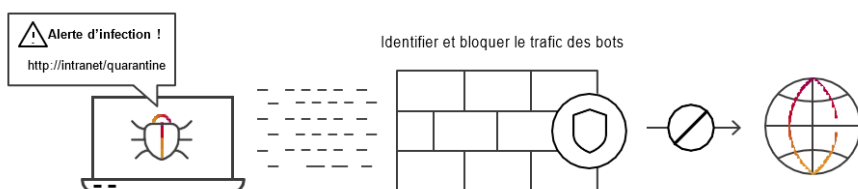


## ESPACES NOMADES

# CONFINEMENT DES BOTS EN TEMPS RÉEL

Protégez votre réseau contre les bots en neutralisant les hôtes infectés par des logiciels malveillants ainsi que l'activité des spams avant qu'ils n'affectent les performances et l'intégrité du réseau. Il faut aussi se prémunir contre les courriers indésirables et le protocole Internet (IP) qui consomme une bande passante précieuse en scannant le trafic de et identifier rapidement les hôtes infectés pour les nettoyer. Les solutions de sécurité Allot surveillent les taux d'établissement des connexions et analysent le comportement anormal des utilisateurs, permettant ainsi aux services informatiques de traiter chirurgicalement le problème à la racine (c'est-à-dire l'hôte infecté par un logiciel malveillant) sans avoir à recourir à des mesures plus larges telles que le blocage de sous-réseaux tout entiers, de liaisons WAN ou de ports. La détection des anomalies basée sur le comportement améliore la sécurité en effectuant un premier "dégraissage" des bots et d'autres logiciels malveillants.

### ALERTE AUX INFECTIONS



### Atouts majeurs

- Protection de l'intégrité du réseau grâce au traitement rapide des infections par les bots
- Productivité garantie de l'entreprise en contenant les hôtes infectés
- Réduction du temps passé par le service d'assistance sur les problèmes résultant de logiciels malveillants

### Confinement des bots en temps réel

- Détection d'un comportement anormal de l'hôte liée aux logiciels malveillants
- Identification de logiciels malveillants via le comportement du réseau (DNS de masse, robots anti-spam et analyse des ports)
- Bloque, limite ou met en quarantaine le trafic utilisateur en quelques secondes
- Informe l'utilisateur et le redirige vers le portail de nettoyage

### Généré par Secure Service Gateway (SSG) d'Allot

- DDoS Secure d'Allot
- Moteur d'analyse du comportement de l'hôte

### Atouts majeurs

- Adaptez le service Wi-Fi à différents groupes de clients et d'employés
- Augmentez vos revenus grâce à des packages Wi-Fi à plusieurs niveaux ainsi qu'à des ventes incitatives en temps réel et post-événement
- Améliorez l'utilisation et la planification des ressources grâce à une visibilité et un suivi complets

### Niveaux de service Wi-Fi en action

- Définissez les niveaux de services par groupe d'utilisateurs
- Appliquez la politique de gestion du trafic de la bande passante à différents niveaux
- Appliquez des plans de service Wi-Fi à plusieurs niveaux et contrôlez en temps réel la congestion de trafic
- Fournissez des rapports d'utilisation détaillés aux clients et à la direction

### Généré par Secure Service Gateway (SSG) d'Allot

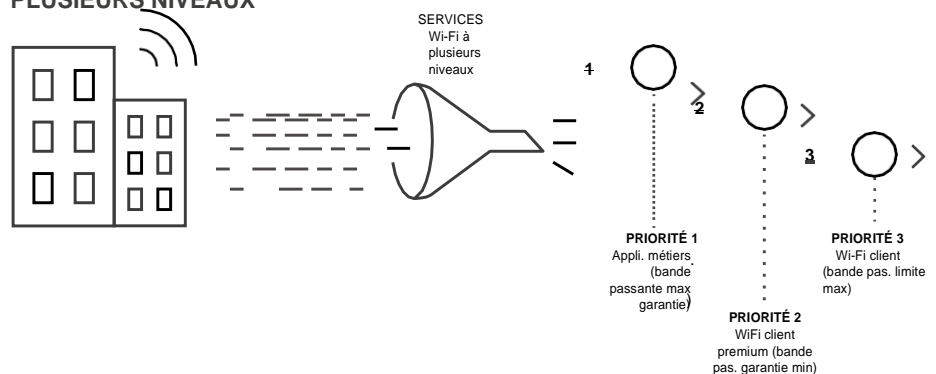
- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot
- Plate-forme de gestion des abonnés Allot

## ESPACES NOMADES

### NIVEAUX DE SERVICE WI-FI

Les hôtels, les aéroports, les centres de congrès et les transports publics desservent souvent différents types de clients et d'employés, à savoir les clients des hôtels, les participants aux congrès, les exposants et le personnel. Les exigences de connectivité Wi-Fi pour ces groupes d'utilisateurs sont généralement assez spécifiques et nécessitent différentes politiques de gestion de la bande passante. Par exemple, les chambres peuvent recevoir une quantité fixe de bande passante Wi-Fi avec une option de paiement supplémentaire, tandis que les zones de congrès et d'exposition affichent la bande passante selon une structure de tarification à plusieurs niveaux par événement. Lors d'un événement tel qu'un salon d'exposition, différentes offres de services Wi-Fi peuvent être proposées, offrant une gamme de vitesses d'accès Wi-Fi, avec des ventes incitatives en temps réel activées par un bureau central de commandement et de contrôle. Dans le même temps, les seuils de congestion sont surveillés, déclenchant des règles de QoS précises qui peuvent limiter le trafic d'égal à égal (P2P) ou les taux d'établissement de connexions individuelles, garantissant une bande passante suffisante pour respecter les accords de niveau de service (SLA).

#### SERVICES WI-FI À PLUSIEURS NIVEAUX





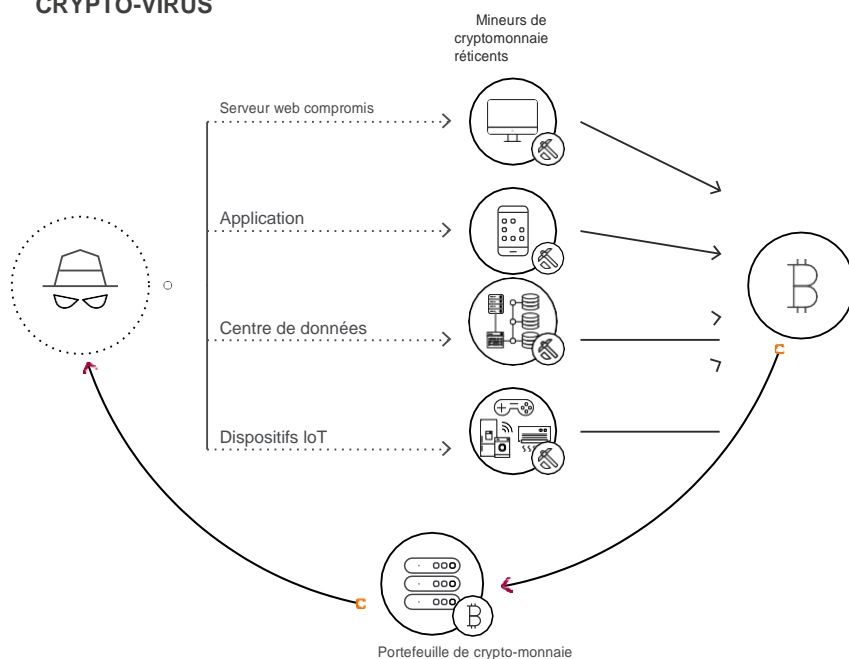
## ESPACES NOMADES

# IDENTIFICATION ET MITIGATION DU CRYPTO-JACKING

Le détournement de crypto-monnaie, ou crypto-jacking, est l'une des principales menaces auxquelles les équipes informatiques d'entreprise sont confrontées aujourd'hui. Alors que le minage de crypto-monnaie nécessite des quantités massives de ressources de traitement informatique, les crypto-jackers ciblent comme moyen d'extraction gratuite la puissance CPU et GPU située dans les entreprises et les organisations.

La surveillance du réseau est certainement le meilleur moyen de se protéger contre le crypto-jacking. Les crypto-jackers doivent pouvoir communiquer avec leurs serveurs cibles, recevoir de nouveaux hachages, les calculer et les renvoyer à leurs propres serveurs. NetworkSecure et Secure Service Gateway d'Allot peuvent identifier cette activité et protéger les précieuses ressources de l'entreprise contre les attaques de crypto-jacking.

### ALERTE D'INFECTION AU CRYPTO-VIRUS



### Atouts majeurs

- Isolation des bibliothèques « Coinhive » qui exploitent la cryptomonnaie « Monero »
- Large reconnaissance et application des politiques de protocoles et d'applications de minage de cryptomonnaie
- Empêche le piratage des ressources du serveur ainsi que l'altération des performances des applications métiers
- Empêche que le précieux matériel réseau soit endommagé par une surchauffe et réduit les coûts de consommation électrique associés au minage de crypto-monnaie

### Identification et mitigation du crypto-jacking

- Identifie et bloque les logiciels malveillants de crypto-monnaie
- Bloque l'accès aux sites web qui injectent le logiciel de minage de crypto-monnaie
- Identifie et bloque les protocoles de minage de crypto-monnaie
- Identifie et bloque le P2P, les VPN et d'autres applications qui activent les attaques de crypto-jacking

### Généré par Secure Service Gateway (SSG) d'Allot

- Sécurité web Allot
- Visibilité et Contrôle Allot

## CONCLUSION

La véritable activité de votre réseau réside dans les processus métiers. La bande passante, le débit, la latence et d'autres mesures de communication courantes sont des aspects de l'évaluation de la façon dont votre réseau prend en charge vos processus internes et externes pour mener à bien votre activité. Et parfois, c'est grâce à votre réseau que l'activité se porte bien.

Comme il est démontré dans les cas d'utilisation présentés dans cette brochure, le SSG d'Allot apporte une forte valeur ajoutée aux opérations, à la planification et à votre entreprise. Tous nos clients ont constaté des avantages immédiats dès qu'ils ont braqué les projecteurs sur leur réseau et ont vu en direct le comportement des applications, des utilisateurs et du réseau. D'après notre expérience, il y a souvent un décalage entre la façon dont les entreprises pensent que leurs processus métiers fonctionnent et la façon dont ils fonctionnent réellement.

En général, la performance des processus métiers laisse à désirer pour les raisons suivantes :

- Le flux des applications qui composent le processus est rompu
- Le réseau connaît des congestions et d'autres problèmes de trafic ou d'équipement
- Des anomalies liées à la sécurité affectent le service ou provoquent un déni de service

Des solutions en termes de visibilité et de contrôle du réseau peuvent mettre en évidence tous ces problèmes en temps réel et fournir les outils nécessaires pour les résoudre. Grâce à nos solutions, votre équipe informatique sera en mesure d'identifier les protocoles et les applications spécifiques, chiffrés ou non, et de surveiller et de mesurer tout élément de politique statique ou dynamique que vous aurez défini.

Le plus apporté par la Visibilité fournira également au service informatique des informations sur la manière d'augmenter les performances du réseau. Par exemple, en voyant quels employés utilisent quelles applications et quand, vous pourrez hiérarchiser le trafic et définir des politiques de gestion du trafic qui répondent à vos objectifs métiers et aux attentes des utilisateurs, ainsi que prendre des décisions en toute connaissance de cause sur la taille et le calendrier des futurs investissements liés au réseau.


Pour plus d'informations, consultez <https://www.allot.com/entreprise> et <https://www.merisac.com>

Contactez MERISAC pour une étude de votre projet  
"See, Control, Secure" dans le Cloud/Datacenter :

[merisac@merisac.com](mailto:merisac@merisac.com)  
Bureau : 01 49 33 737 5  
Mobile : 06 60 12 64 51

**MERISAC**  
INSTRUMENTS  
Intégrateur de Services WAN & Datacenter

Traduction française assurée par les sociétés

 translated.

**MERISAC**  
INSTRUMENTS  
Intégrateur de Services WAN & Datacenter

**allot**



© 2018 Allot Ltd. Tous droits réservés. Allot Ltd, Sigma, NetEnforcer et le logo Allot sont des marques commerciales d'Allot Ltd. Tous les autres noms de marques ou de produits sont des marques déposées de leurs détenteurs respectifs. Les informations contenues dans ce document sont fournies à titre indicatif uniquement et ne constituent ni une offre, ni un engagement, ni une acceptation. Allot peut modifier les informations à tout moment sans préavis.

[www.allot.com](http://www.allot.com)