

Allot SmartSentinel

La solution de mise en conformité numérique

Introduction

Sauvegarder le cyber-espace national, s'assurer de la souveraineté numérique et conserver un certain contrôle sur le réseau du pays sont autant d'aspects critiques pour les gouvernements de tous les pays du monde.

Allot SmartSentinel permet aux organismes gouvernementaux d'accroître la visibilité du trafic sur le réseau national et de le contrôler via la conformité numérique pour faire respecter les lois et les politiques nationales.

Voir tout le trafic sur le réseau au niveau national, régional ou utilisateur. **Contrôler** Internet, les applications ainsi que les activités liées aux médias sociaux. **Garantir** et protéger les ressources stratégiques et l'infrastructure nationale contre les cyberattaques.

Allot SmartSentinel est une solution flexible, puissante et évolutive qui offre une protection contre les menaces actuelles et futures via un processus d'apprentissage automatique, d'identification dynamique des menaces et d'autres technologies avancées.

Solution

Allot SmartSentinel est une solution spécialement conçue pour permettre aux organismes d'application de la loi, de sécurité nationale et aux autres organismes gouvernementaux de satisfaire les exigences de sécurité nationale en faisant appliquer les politiques et la réglementation dans tous les réseaux de télécommunications.

Grâce à sa plate-forme centralisée, Allot SmartSentinel dispose de la puissance nécessaire pour inspecter des téraoctets par seconde de données et stocker ou transmettre des pétaoctets de données d'application et de données utilisateurs.

Avantages

Allot propose une solution unique et unifiée, basée sur une protection en ligne massivement évolutive qui inspecte chaque paquet et offre les avantages clés suivants :

- Visibilité granulaire des mégadonnées relatives au comportement sur le réseau des utilisateurs et des applications pour prendre en charge et faire appliquer les lois et réglementations
- Capacités de blocage : contenus illégaux, pornographiques, violents, liés à la drogue et la maltraitance des enfants, contenus faux et mensongers et applications illégales
- Conservation ou transmission illimitée des enregistrements détaillés des données d'utilisation
- Protection de l'infrastructure réseau contre les attaques de DDoS
- Identification et atténuation de l'utilisation illégale de la VoIP

Fonctionnalité complète



SEE

- Visibilité complète du réseau IP, chiffrement équivalent des données et des applications jusqu'au niveau utilisateur
- Analyse automatique et classification de l'application, de l'utilisateur, de la session, de l'appareil, de l'emplacement, du contenu, du type d'intérêt, etc.
- Visibilité détaillée et complète des serveurs proxy anonymes, VPN, accès au darknet et activités liées aux cryptomonnaies
- Conservation des données : collecte de tous les enregistrements de métadonnées



CONTROL

- Classification /filtrage Web et du contenu : pédophilie, violence, jeux de hasard, drogue, etc. (prise en charge de la liste noire de l'International Watch Foundation)
- Blocage, redirection et interruption du trafic vers/ en provenance de sites et applications spécifiques
- Surveillance/blocage des VPN et serveurs proxy anonymes
- Blocage des activités liées aux cryptomonnaies
- Redirection sélective du trafic suspect pour inspection approfondie, notamment le protocole TLS/SSL
- Isolement des protocoles et hiérarchisation du trafic en cas d'urgence



SECURE

- Cybersécurité du réseau au niveau de l'état (anti-logiciels malveillants/antivirus, antihameçonnage)
- Blocage de l'accès au darknet
- Détection DDoS et atténuation des attaques entrantes et sortantes volumétriques
- Détection des activités de botnet et confinement
- Renseignements détaillés sur les menaces liées aux cybercriminels et à leurs cibles sur le réseau
- Garantie d'un réseau sûr pour les organes et services gouvernementaux

Prêt à l'action

Allot SmartSentinel prend en charge les principaux cas d'utilisation :

- Filtrage Web (URL/domaine) et de contenu conformément aux exigences réglementaires, par exemple : maltraitance des enfants, pornographie, drogue, jeux de hasard, etc.
- Capacité à bloquer ou interrompre tout service d'une application utilisée dans le cadre d'activités illégales
- Détection et désactivation de l'utilisation des serveurs proxy anonymes suspects et de l'activité des VPN
- Divulgarion de l'accès utilisateur au darknet
- Conservation des données : collecte et conservation ou transmission des métadonnées pour les besoins des enquêtes liées à l'application de la loi
- Détection DDoS au niveau national et atténuation des attaques entrantes et sortantes volumétriques
- Cybersécurité du réseau au niveau de l'état (anti-logiciels malveillants/virus, anti-bot, anti hameçonnage) dédiée aux organisations ou aux utilisateurs

À propos d'Allot

Allot (NASDAQ, TASE: ALLT), depuis sa fondation en 1996, est un leader mondial dans le domaine des solutions innovantes d'intelligence réseau et de sécurité dédiées aux fournisseurs de services de communication (CSP) ainsi qu'aux entreprises du monde entier. Nous donnons à nos clients la possibilité de contrôler la réglementation, les règles et les lois et de les transformer en politiques réseau concrètes et applicables destinées à garantir la cybersécurité ainsi que la sécurité nationale. Grâce à nos 25 années d'expérience reconnue, nos solutions de mise en conformité numérique vont transformer votre réseau, vos applications, votre utilisation et vos données de sécurité en renseignements concrets permettant d'assurer la sécurité du pays, des réseaux et de protéger les utilisateurs.

Pour en savoir plus à propos des solutions dédiées au secteur public, veuillez nous contacter à l'adresse suivante :

Allot ltd | digital.enforcement@allot.com

