Illumio

La plateforme de segmentation zero trust

Une Plateforme. Une console. Tous les environnements

L'explosion de la surface d'attaque des entreprises hybrides modernes rend les brèches inévitables malgré tous les efforts possibles en prévention et en détection. La diminution drastique des risques et des conséquences passe par une approche Zero Trust d'une part et par l'acceptation de la brèche d'autre part. Contenir au maximum cette brèche inéluctable est devenu le nouveau paradigme.

Pour savoir comment éviter qu'une attaque ransomware ne devienne un véritable désastre, **consultez le livre blanc** :

MIEL

Distribué en France par MIEL
01 60 19 34 52 - www.miel.fr

Illumio, “the Zero Trust Segmentation company” (ZTS), empêche la propagation des brèches et des ransomwares sur toute la surface d’attaque hybride. La plateforme ZTS Illumio visualise tous les flux de trafics entre les workloads ou les équipements et cloisonne les communications entre les ressources en fonction de leur rôle et de leur exposition. Elle isole les actifs critiques ainsi que les systèmes compromis, en prévention ou en réponse à une attaque active. Ce type de segmentation est la fondation et un pilier stratégique de toute architecture Zero Trust

1. Voir et identifier les risques

Une visibilité sans précédent cartographie toutes les communications et le trafic entre les workloads et les devices sur toute la surface d’attaque

2. Mettre en place les règles

Des politiques flexibles et granulaires de segmentation contrôlent les communications entre les workloads et les devices pour «fermer les portes» et n’autoriser que les communications nécessaires et désirées

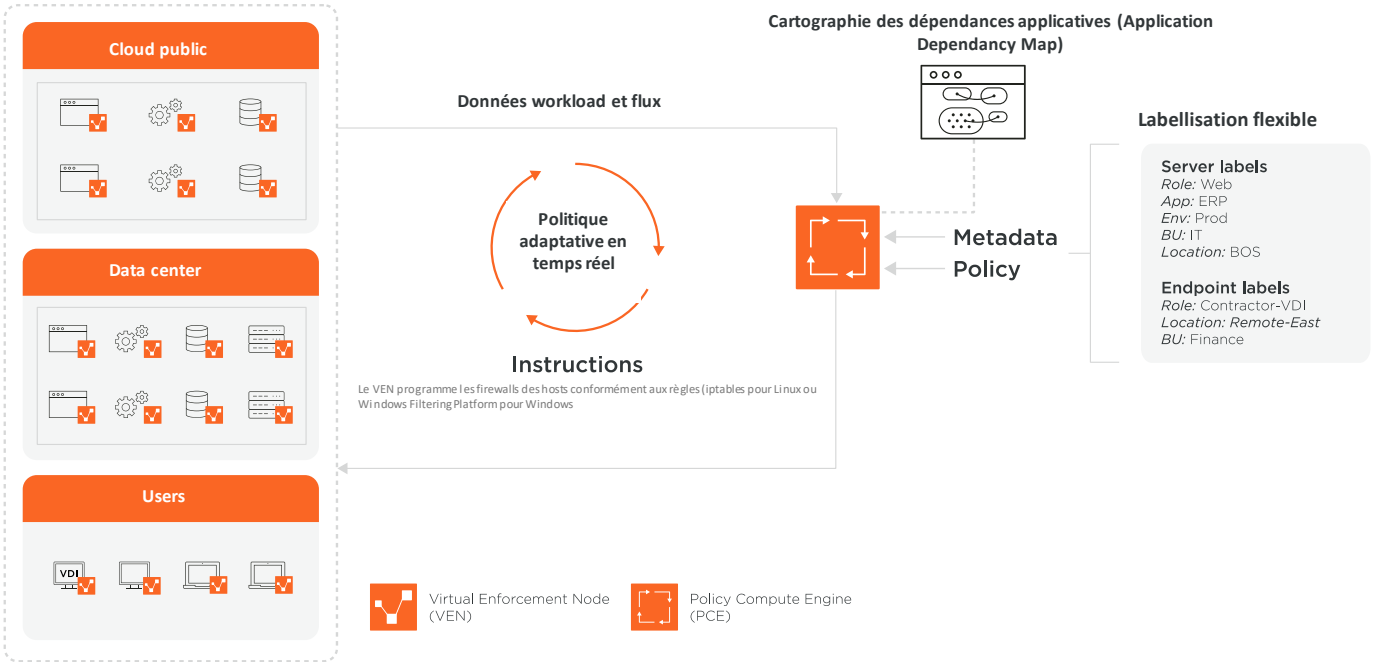
3. Arretêr la propagation

Contrôle la communication latérale « est-ouest ». Sanctuarise en prévention les actifs critiques ou isole réactivement les actifs compromis

Architecture Illumio : Rapide, Simple, Evolutif

L’architecture logicielle Illumio possède simplement 2 composantes clés :

- Un agent léger s’installant sur les workloads (VM, Node Container, serveur physique) et/ou les endpoints : Le VEN (Virtual Enforcement Node)
- Un moteur d’administration centralisée et de monitoring : le PCE (Policy Compute Engine)



Associées à un système de labélisation des hosts, ces 2 composantes permettent :

- **Une cartographie complète des flux**, grâce à la télémétrie remontée par les agents vers le PCE.
- **Une politique granulaire de segmentation totalement découplée du réseau et de ses changements**, appliqué dynamiquement par le PCE vers les VEN, et qui a pour objectif final de bloquer tout flux non explicitement autorisé.

Les agents utilisent les solutions natives de sécurité des hosts (Windows filtering platform, Iptable…) pour appliquer les règles établies.

Avantages clés

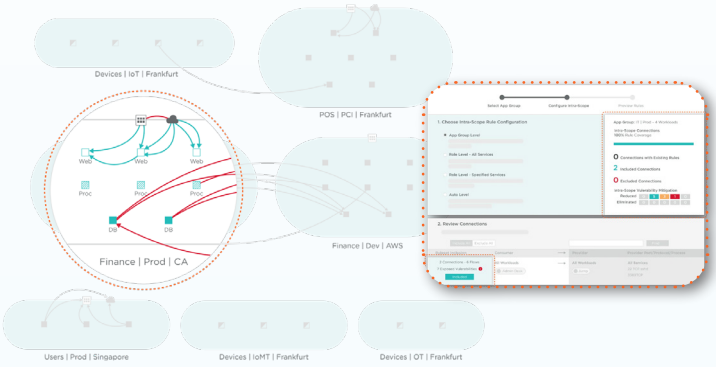
Rendre le Zero Trust possible	Renforcer la cyber résilience	Confiner rapidement les brèches	Simplifier la visibilité
Illumio supporte tous les piliers de Zero Trust, protégeant les données, users, devices, workloads, et réseaux • Vérification continue basée sur les risques • Applique les accès de moindre privilège • Monitoring global de la sécurité	Prévenir et préparer les systèmes et réseaux en cas de compromission de la sécurité. • Implémenter des contrôles granulaires pour limiter l'étendue de l'attaque • Identifier les zones à haut risque • Bâtir une protection à long terme	Appliquer les principes Zero Trust pour se concentrer sur le confinement, pas seulement la prévention et la détection • Stoppe la propagation des ransomwares • Met rapidement en quarantaine les systèmes compromis • Accélère la réponse avec des alertes automatisées	Obtenir en quelques secondes une vue détaillée de tous les flux de trafic entre les workloads. • Identifier et évaluer les schémas de flux applicatifs • Découvre rapidement le shadow IT • Analyse les flux et leurs schémas en fonction de la conformité

Produits

Illumio Core

Segmentation Zero trust pour les workloads de tous les Data Center (On-premise et cloud)

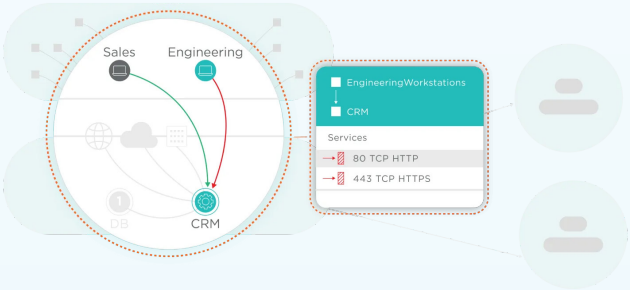
Le trafic est visible pour toutes les workloads comme les VM, les containers et l'IT/OT sur une même console. Une segmentation à toutes les échelles, de l'emplacement au service, permet de contenir la propagation de la brèche en prévenant le mouvement latéral indépendamment de l'architecture, de la taille ou de la complexité du Data Center. Une interface utilisateur très intuitive permet de déployer des règles granulaires en quelques minutes et de faire un suivi guidé exhaustif de la résilience à la suite d'une compromission



Illumio Endpoint

Segmentation des équipements utilisateurs

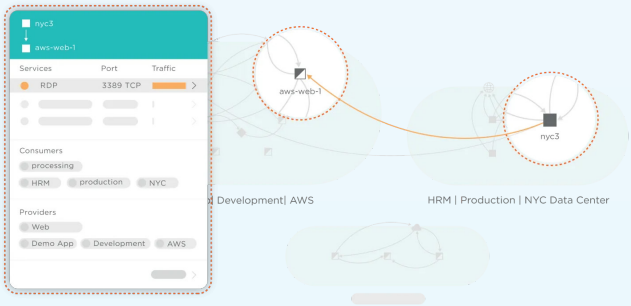
Illumio Endpoint visualise le trafic réseau d'un endpoint où qu'il se trouve pour évaluer ses risques. Les accès des utilisateurs ne sont autorisés que pour les applications légitimes. En complément d'un EDR (Endpoint Detection and Response) qui résout la compromission, Les attaques sont confinées à un équipement unique avant même qu'elle ne soit détectée par d'autres solutions de sécurité



Illumio CloudSecure

Visibilité et contrôles sans agent et multicloud

Illumio CloudSecure se connecte facilement aux comptes PaaS AWS et Azure pour collecter et consolider des métadonnées et une télémétrie du trafic en temps réel. Ces données temps réel sont le moteur d'une politique de cloisonnement visant à protéger les actifs critiques des menaces du cloud



Contactez-nous
+33 1 60 19 34 52
reseausecu@miel.fr

Voir la page produit :