illumio

EXPOSÉ TECHNIQUE

Architecture Illumio

Développez rapidement la cyber-résilience de votre organisation avec la segmentation Zero Trust (ZTS) dans votre cloud, votre centre de données et vos postes de travail fixes ou nomades

Présentation architecturale

Avec Illumio, vous pouvez rationaliser votre chemin vers la sécurité Zero Trust pour défendre votre organisation contre les menaces de sécurité croissantes d'aujourd'hui.

Illumio offre une segmentation Zero Trust de pointe dans le secteur qui permet une visibilité unifiée et des contrôles par liste d'autorisation/de refus. Illumio comprend les trois composants suivants :

Moteur de calcul des politiques (PCE)

Le PCE est la console de gestion Illumio et le contrôleur de segmentation. Il collecte en permanence des informations de télémétrie à partir du VEN, fournissant une cartographie en temps réel des modèles de trafic et recommandant des règles d'autorisation optimales basées sur des informations contextuelles sur l'environnement, les charges de travail et les processus.

Agent Illumio Virtual Enforcement Node (VEN)

Le VEN est un agent léger qui est installé dans le système d'exploitation d'un serveur ou d'un poste de travail Il collecte les informations de flux et de métadonnées et les transmet au PCE. Il reçoit également les règles de pare-feu du PCE pour programmer le pare-feu L3/L4 intégré au système d'exploitation. De manière essentielle, L'agent Illumio VEN ne fait pas de redirection de trafic. Il n'est pas le pare-feu et n'achemine pas le trafic.

L'innovation en un coup d'œil

Avec Illumio, vous pouvez contenir les rançongiciels, établir la cyber-résilience et empêcher les violations de se transformer en cyber-catastrophes.

Mise en application automatisée de la sécurité

Mettre en vigueur immédiatement les règles par listes d'autorisation/refus.

Affichage en temps réel des flux de communication des applications

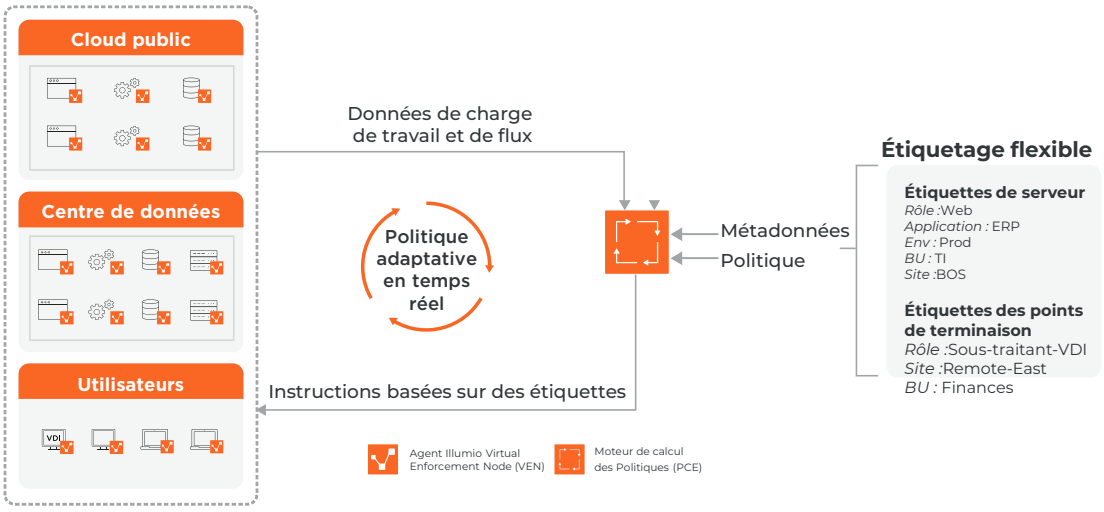
Visualisez facilement tous vos flux de trafic et connaissez leurs risques potentiels.

Sécurité multi-cloud à grande échelle

Appliquer continuellement la sécurité des charges de travail sur les clouds ou les centres de données

Contrôler le trafic des postes de travail

La prise en charge hors domaine vous permet de déployer la segmentation au-delà du périmètre réseau traditionnel.



Visibilité sans agent et mise en vigueur de la segmentation

Dans les environnements où des agents ne sont pas déployés (tels que les systèmes hérités, IoT/OT et les objets cloud comme AWS RDS), Illumio ingère des données de flux à partir de l'équipement réseau (routeurs, commutateurs, équilibreurs de charge), des métadonnées d'objet cloud, des informations de groupe de sécurité natives cloud et des journaux de flux.

Cette télémétrie fournit une carte unifiée des flux de communication dans votre infrastructure numérique.

Pour segmenter, Illumio génère des ACL (listes de contrôle d'accès) des routeurs, commutateurs et équilibreurs de charge. Et pour le cloud, il recommande et programme des politiques pour optimiser les groupes de sécurité natifs du cloud.

Capacités essentielles

Cartographie des dépendances applicatives

Visualisez les informations en temps réel dans les flux de communication des applications. Cela vous aide à comprendre les chemins critiques, à détecter les comportements anormaux, à créer des politiques de segmentation et à tester les règles avant de les déployer.

Règles d'autorisation et de déni

Des règles faciles à écrire utilisant un langage naturel qui aident les organisations à progresser efficacement et en toute sécurité vers la ZTS tout en évitant la complexité des modèles traditionnels.

Générateur de politiques

L'historique des flux est utilisé pour créer et recommander des stratégies de segmentation optimales pour les charges de travail, quel que soit leur emplacement ou leur type. Créez des stratégies sans connaître les éléments réseau telles que les adresses IP, les sous-réseaux et les VLAN.

Prise en charge hors domaine

La segmentation d'Illumio n'est pas liée au réseau. Ainsi, la politique peut être appliquée pour un appareil où qu'il soit. La police est automatiquement mise à jour en fonction de l'emplacement de l'appareil pour une couverture de segmentation optimale.

Cartes de vulnérabilité

Les cartes de vulnérabilité combinent ZTS avec les données de vulnérabilité provenant des outils d'analyse. Obtenez une connaissance détaillée des voies de déplacement latéral potentiellement utilisables par les malwares et les pirates informatiques.

Chiffrement de charge de travail à charge de travail

SecureConnect prend en charge le chiffrement du trafic hôte-hôte à la demande entre les charges de travail appariées en utilisant les bibliothèques de chiffrement intégrées aux systèmes d'exploitation hôtes. SecureConnect est basé sur des politiques et géré par le PCE.

Spécifications du produit

Prise en charge de la plateforme

- Illumio VEN fonctionne sous Windows, macOS et Linux. Avec une large prise en charge des versions, Illumio peut fournir une couverture dans pratiquement n'importe quel environnement.
- Charges de travail sans agent sécurisées avec CloudSecure et NEN
- Prenez en charge les déploiements de conteneurs via le VEN conteneurisé d'Illumio pour les principales plateformes d'orchestration telles que Kubernetes et OpenShift.

Pour une liste à jour des systèmes d'exploitation et conteneurs pris en charge, consultez support.illumio.com.

Intégration technique

Illumio s'associe aux plus grandes sociétés de logiciels, d'infrastructure et de sécurité pour fournir des solutions intégrées et interopérables qui soutiennent votre stratégie Zero Trust. Découvrez nos dernières intégrations sur illumio.com/partners/tap.

Des informations détaillées sur les produits Illumio sont disponibles sur docs.illumio.com.

Illumio propose des options de déploiement sur site et dans le cloud. Illumio fournit un accord de niveau de service (SLA) de 99,8 % pour Illumio Core, Endpoint et Edge SaaS PCE. Pour plus d'informations sur le SLA, consultez le Contrat-cadre d'abonnement Illumio (www.illumio.com/eula).

À propos d'Illumio

Illumio, pionnier et leader du marché de la segmentation Zero Trust, empêche les violations de devenir des cyber-catastrophes. Illumio protège les applications critiques et les actifs numériques précieux grâce à une technologie de segmentation éprouvée, spécialement conçue pour le modèle de sécurité Zero Trust. Les solutions d'atténuation et de segmentation des rançongiciels Illumio détectent les risques, isolent les attaques et sécurisent les données sur les applications natives du cloud, les clouds hybrides et multiclouds, les centres de données et les terminaux, permettant ainsi aux plus grandes organisations mondiales de renforcer leur cyber-résilience et de réduire les risques.