illumio

INFOS PRODUIT

La plateforme de segmentation Zero Trust d'Illumio

Une seule plateforme. Une seule console. N'importe quel environnement.

Confinement des violations. Le nouveau paradigme.

La surface d'attaque ne cesse de grandir

Au cours des deux dernières années, les attaques de rançongiciel sont devenues de plus en plus fréquentes, arrivant toutes les 11 secondes et affectant 76 % des organisations. Cela souligne le défi important auquel sont confrontés les RSSI et les équipes sécurité et TI, alors que les environnements passent de sur site à un paysage hyperconnecté, hybride, en premier lieu sur le cloud. La surface d'attaque grandissante suscitée par la transformation numérique augmente le risque pour toutes les organisations.

L'expansion des SI hybrides introduit des lacunes significatives dans la surface d'attaque. Les attaquants se régalent dans un paysage comprenant de multiples points de terminaison, centres de données, conteneurs, machines virtuelles, mainframes, environnements de production et de développement, technologies opérationnelles (TO du SII - Systèmes d'Information Industriels) etc.

La seule solution qui gère la communication sur tous les types de charges de travail

La plateforme Zero Trust Segmentation (ZTS) d'Illumio est la seule solution capable de tout gérer : Point de terminaison à point de terminaison, point de terminaison à serveur, serveur à serveur, ainsi qu'une prise en charge étendue des charges de travail cloud, des conteneurs, des appareils IdO et TO. Ainsi les organisations peuvent être plus résilientes face à toute éventualité.

Cette approche innovante et cette visibilité inégalée nous permettent de passer de la mentalité « trouver et réparer » à la réalité « limiter et contenir ». Illumio utilise les informations dans les flux de trafic pour appliquer les principes Zero Trust afin de se concentrer sur le confinement des violations, et pas seulement sur la prévention et la détection.

Principaux avantages

Voir risque

Une visibilité inégalée permet de visualiser l'ensemble de la communication et du trafic entre les charges de travail et les appareils dans la surface d'attaque hybride.

Définir la politique

Définissez des stratégies de segmentation granulaires et flexibles qui contrôlent la communication entre les charges de travail et les appareils pour ne permettre que ce qui est nécessaire et souhaité.

Arrêter la propagation

Clôturez de manière proactive les ressources de grande valeur ou isolez de manière réactive les systèmes compromis pendant une attaque de façon à arrêter la propagation d'une violation.

Protégez vos charges de travail avec la première plateforme du secteur pour le confinement des violations

Contrairement aux technologies de prévention et de détection, ZTS contient la propagation des violations et des rançongiciels à travers la surface d'attaque hybride en visualisant continuellement la manière dont les charges de travail et les appareils communiquent, en créant des stratégies granulaires qui ne permettent que la communication souhaitée et nécessaire, et en isolant automatiquement les violations en limitant les mouvements latéraux de manière proactive ou pendant une attaque active. ZTS est un pilier fondamental et stratégique de toute architecture Zero Trust.

Couverture complète de la surface d'attaque

La définition du périmètre devient de moins en moins claire à mesure que les points de terminaison se connectent à partir de divers emplacements, que les charges de travail des serveurs sont réparties entre le centre de données et le cloud, et que le nombre d'appareils IdO (Internet des objets) et TO (technologie opérationnelle) continue d'augmenter.

Pour une couverture complète de la surface d'attaque moderne, Illumio ne couvre pas seulement les ressources et les points de terminaison traditionnels sur site. Il peut également segmenter et protéger des ressources sans agent tels que des systèmes hérités, l'IdO et la TO, et des charges de travail cloud, éliminant ainsi les silos et améliorant la cyber-résilience.

Capacités critiques

Activer Zero Trust

Illumio ZTS prend en charge tous les piliers de Zero Trust, en protégeant les données, les utilisateurs, les appareils, les charges de travail et les réseaux.

- Maintenir une vérification continue basée sur les risques
- Appliquer l'accès le moins privilégié
- Bénéficier d'une surveillance de sécurité complète

Renforcer la cyber-résilience

Soyez prêts et évitez le déraillement de systèmes et de réseaux si la sécurité est compromise.

- Mettez en œuvre des contrôles granulaires pour limiter la portée des attaques
- Identifiez les zones à haut risque
- Construisez une protection à long terme

Confiner les violations en quelques minutes

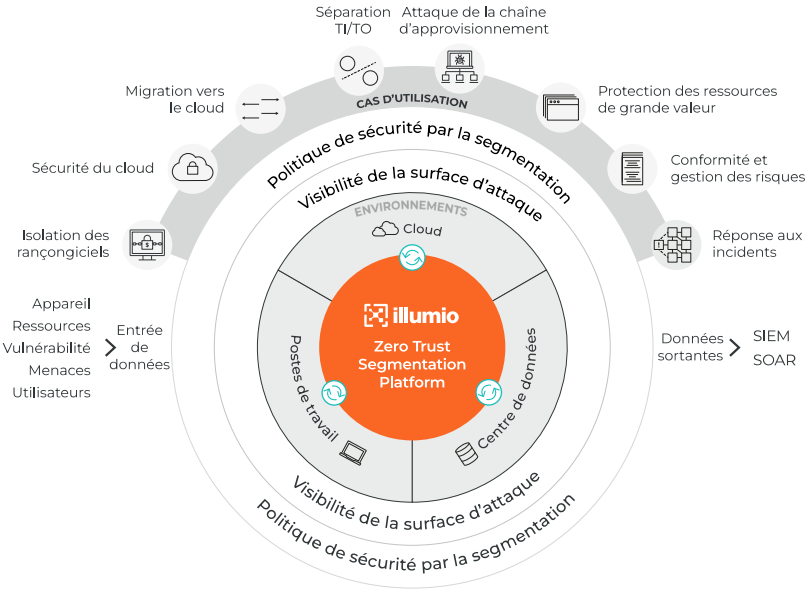
Appliquez les principes Zero Trust pour vous concentrer sur le confinement, pas seulement sur la prévention et la détection.

- Empêcher le rançongiciel de se propager
- Mettre rapidement en quarantaine les systèmes compromis
- Réponse rapide avec alertes automatisées

Visibilité facilitée

Obtenez une vue complète et détaillée de tous les flux de trafic entre charges de travail en quelques secondes.

- Identifiez les risques en évaluant les modèles de trafic actuels
- Découvrez rapidement les systèmes informatiques fantômes
- Analysez les flux de trafic et les modèles de conformité aux politiques



À propos d'Illumio

Illumio, la société de segmentation Zero Trust, empêche les failles de sécurité et les rançongiciels de se propager à travers la surface d'attaque hybride. La plateforme Illumio ZTS visualise tout le trafic entre les charges de travail, les systèmes et Internet, définit automatiquement des stratégies de segmentation granulaire pour contrôler les flux de données et isole les actifs de grande valeur et les systèmes vulnérables, soit de manière proactive, soit en réponse à des attaques actives. Illumio protège les organisations de toutes tailles, des Fortune 100 aux PME, en stoppant les failles de sécurité et les rançongiciels en quelques minutes et en accélérant les projets de transformation numérique et cloud, de manière à leur permettre d'économiser des millions de dollars occasionnés par l'indisponibilité des applications.

Copyright © 2023 Illumio, Inc. Tous droits réservés. Illumio® est une marque commerciale ou une marque déposée d'Illumio, Inc. ou de ses filiales aux États-Unis et dans d'autres pays. Les marques commerciales tierces mentionnées dans ce document appartiennent à leurs propriétaires respectifs.