Illumio Segmentation

Contrôlez les mouvements latéraux pour empêcher les vols de données et les attaques par ransomware d'aboutir et de devenir de véritables catastrophes.

Une nouvelle forme de segmentation pour des réseaux nouvelle génération

Des réseaux toujours plus vastes, hybrides et en constante évolution – voilà un environnement idéal pour les cyber-attaquants.

Rien que l'année dernière, 88 % des organisations ont été touchées par des ransomwares, et 58 % d'entre elles ont dû interrompre leurs opérations.

Avec l'apparition d'environnements hybrides et multi-cloud, du télétravail et des applications distribuées, les périmètres traditionnels ont tout simplement disparu et des interactions complexes apparaissent, qui peuvent favoriser les attaquants.

Une fois les ceux-ci infiltrés, ils se propagent rapidement dans le réseau et compromettent discrètement les données et systèmes critiques. Ce mouvement latéral est difficile à détecter, rendant les violations plus fréquentes, sophistiquées et destructrices. Les experts en cybersécurité s'accordent à dire qu'une approche Zero Trust fondée sur la segmentation est la meilleure façon de contenir les violations, de réduire les risques et de renforcer la résilience. La segmentation Illumio vous permet d'obtenir une visibilité granulaire du trafic réseau, de maîtriser les vulnérabilités, de stopper les mouvements latéraux non autorisés et de contenir les violations — dans le cloud, les datacenters ou sur les endpoints.

Principaux avantages

Visibilité complète et granulaire

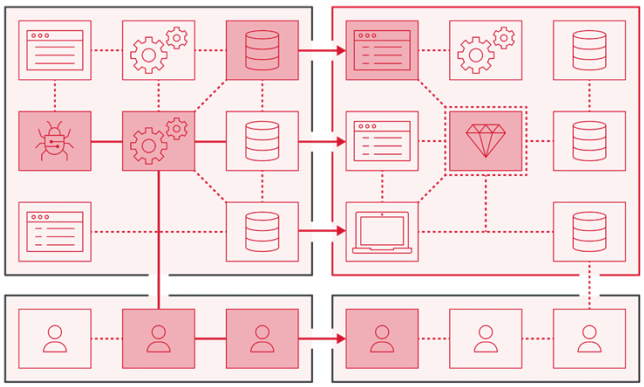
Cartographiez les communications entre workloads. Identifiez les risques cachés, puis créez des politiques qui bloquent automatiquement les chemins classiques empruntés par les ransomwares pour empêcher leur propagation.

Segmentation simplifiée

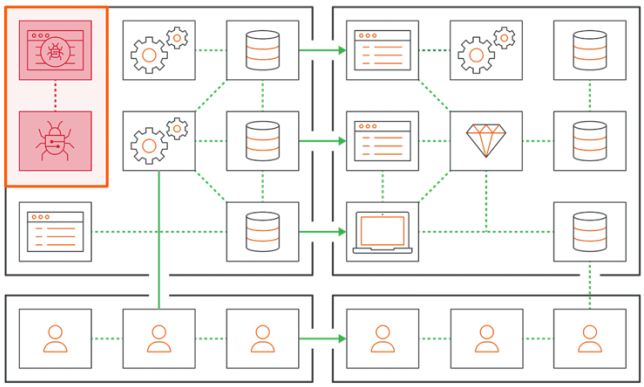
Segmentez tous les workloads — dans le cloud, sur les endpoints et dans les datacenters. Empêchez la propagation des violations. Isolez les systèmes compromis. Bénéficiez d'une segmentation qui évolue avec vos besoins.

Zero Trust sans complexité

La segmentation est la base de toute stratégie Zero Trust. Appliquez le principe du moindre privilège. Supprimez la confiance implicite dans vos environnements hybrides et multi-cloud.



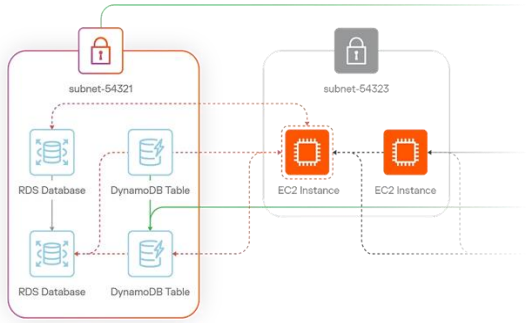
Sans segmentation, les violations se propagent rapidement



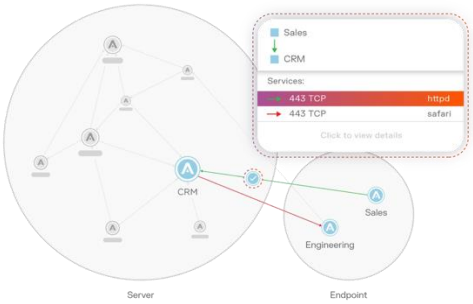
Avec la segmentation, les brèches sont contenues et détectées

Une solution de segmentation pour chaque environnement

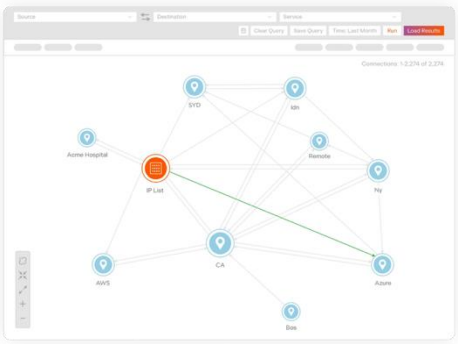
Peu importe où résident vos workloads — dans le cloud, sur les endpoints ou dans les datacenters — la segmentation Illumio offre une solution unifiée cohérente, simple et évolutive. C'est une solution qui met fin aux outils cloisonnés et qui permet d'adopter une sécurité Zero Trust unifiée et adaptée à l'ensemble de votre environnement. Illumio Segmentation permet de contenir les violations dans les datacenters sur site, les conteneurs, les environnements IT/OT et les machines virtuelles. Visualisez tout le trafic, quelle que soit l'architecture, la taille ou la complexité de votre réseau. Segmentez les workloads sans perturber les opérations.



Contenir les attaques cloud à leur source
Visualisez les applications cloud, les ressources, les flux de trafic et les métadonnées. Mettez en place une segmentation cohérente et dynamique dans des environnements hybrides, multi-cloud et conteneurisés.



Contenir les violations sur un poste de travail, un ordinateur portable ou une machine virtuelle
Et ce, avant même qu'elles ne soient détectées par d'autres outils de sécurité. Visualisez les communications réseau entre les terminaux et les applications, et appliquez le principe du moindre privilège.



Contenir les violations sur un poste de travail, un ordinateur portable ou une machine virtuelle
Et ce, avant même qu'elles ne soient détectées par d'autres outils de sécurité. Visualisez les communications réseau entre les terminaux et les applications, et appliquez le principe du moindre privilège.

Un graphe de sécurité basé sur l'IA

La plateforme Illumio repose sur un graphe de sécurité basé sur l'IA, offrant une vue en temps réel inégalée de votre surface d'attaque.

Illumio Insights et Illumio Segmentation collaborent pour fournir une solution complète de confinement des violations.

Illumio Insights fournit des informations basées sur l'AI Cloud Detection and Response (CDR), qui identifie les risques de mouvement latéral, détecte les attaques en cours et contient les menaces en un clic — à l'échelle du cloud.

Illumio Segmentation vous aide à visualiser rapidement les risques et à définir des politiques pour empêcher la propagation des violations.

Isolez les incidents avec Illumio Segmentation

Illumio.com/illumio-segmentation

À propos d'Illumio

Illumio est le leader du confinement des ransomwares et des brèches de sécurité, redéfinissant la manière dont les organisations contiennent les cyberattaques et assurent leur résilience opérationnelle. Propulsée par l'IA Security Graph, la plateforme de confinement d'Illumio identifie et isole les menaces dans les environnements hybrides et multi-cloud, empêchant ainsi la propagation des attaques avant qu'elles ne provoquent des catastrophes.

Reconnue comme leader dans le rapport Forrester Wave™ sur la microsegmentation, Illumio permet l'implémentation du modèle Zero Trust et renforce la résilience cyber des infrastructures, systèmes et organisations.