Illumio Segmentation

Contrôlez les déplacements latéraux pour éviter que les compromissions et les attaques par ransomware ne deviennent des incidents majeurs.

Segmentation moderne pour les réseaux d'aujourd'hui

Les réseaux tentaculaires, hybrides et en constante évolution d'aujourd'hui réunissent les conditions parfaites pour lancer des attaques.

Au cours de la seule année dernière, 88 % des entreprises ont été victimes de ransomwares et 58 % d'entre elles ont été contraintes d'interrompre leur activité à la suite de ces attaques.

Dans un monde caractérisé par les environnements multicloud hybrides, le télétravail et les applications distribuées, force est de constater que les périmètres traditionnels ont disparu depuis longtemps.

Une fois infiltrés, les cybercriminels peuvent se propager rapidement au sein de votre réseau et infecter silencieusement les systèmes et données critiques. Ce type de déplacement latéral est difficile à détecter, ce qui contribue à l'augmentation des compromissions, mais aussi à leur sophistication et à leur potentiel de destruction.

Les experts en cybersécurité reconnaissent qu'une approche Zero Trust basée sur la segmentation est le moyen le plus efficace pour confiner les compromissions, réduire les risques et renforcer la résilience.

Illuminio Segmentation vous offre le contrôle nécessaire pour bénéficier d'une visibilité granulaire sur le trafic réseau, corriger les vulnérabilités, bloquer les déplacements latéraux non autorisés et confiner les compromissions — dans le cloud, les centres de données ou sur les terminaux.

Principaux avantages

Visibilité granulaire complète

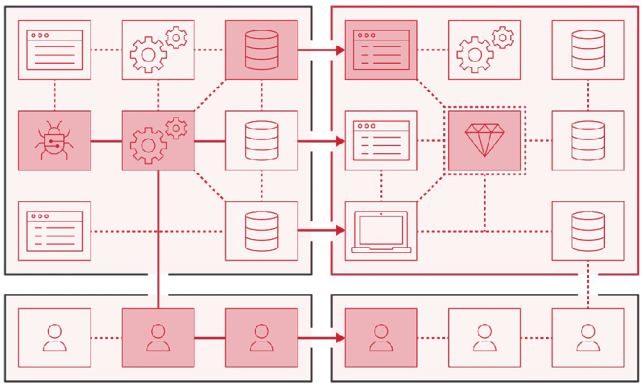
Cartographiez les communications associées aux charges de travail. Mettez au jour les risques cachés, puis créez des stratégies qui bloquent automatiquement les trajets habituels des ransomwares pour éviter toute propagation.

Segmentation simplifiée

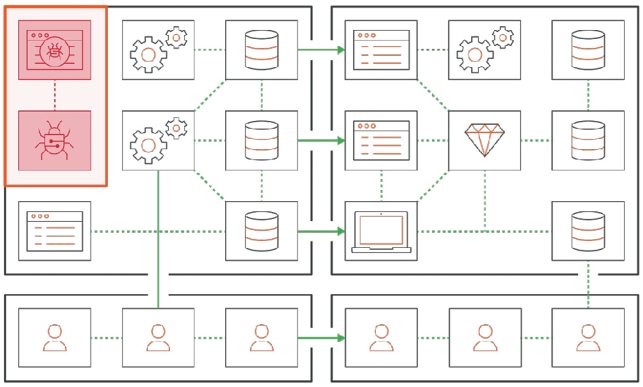
Segmentez toutes les charges de travail exécutées dans le cloud, sur les terminaux et dans les centres de données. Empêchez la propagation des compromissions. Isolez les systèmes compromis. Bénéficiez d'une segmentation qui évolue en fonction des besoins de votre entreprise.

Le Zero Trust en toute simplicité

La segmentation est la base de toute stratégie Zero Trust. Appliquez le principe du moindre privilège. Éliminez la confiance implicite dans les environnements multicloud hybrides.



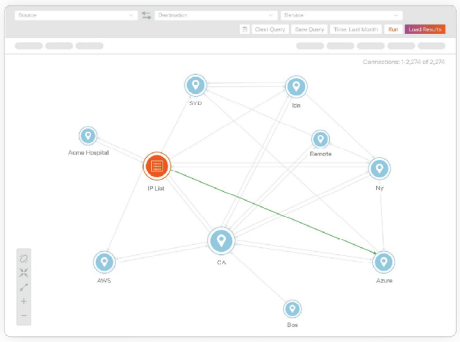
Sans segmentation, les compromissions se propagent rapidement.

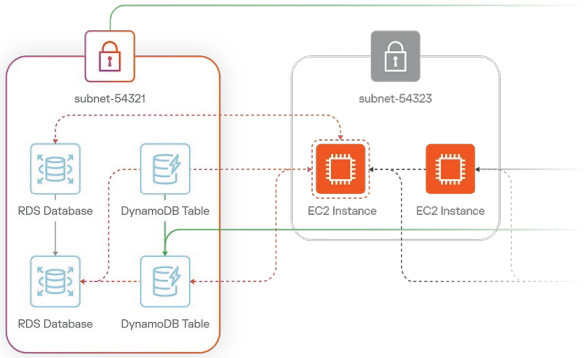


Avec segmentation, elles sont rapidement détectées et confinées.

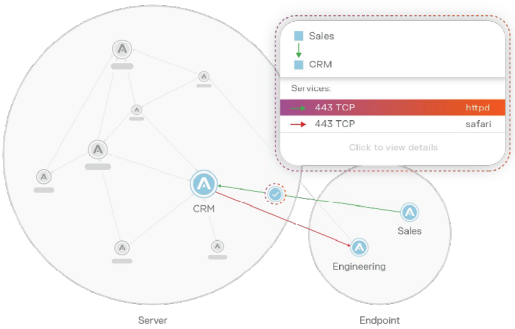
Une solution de segmentation pour chaque environnement

Quel que soit l'emplacement de vos charges de travail — dans le cloud, les centres de données ou sur les terminaux —, Illumio Segmentation vous offre une solution simple, cohérente et évolutive. Dites adieu aux outils cloisonnés et offrez-vous une sécurité Zero Trust unifiée, adaptée à tout votre environnement.





Confinez les attaques cloud à la source. Visualisez les applications, ressources, flux de trafic et métadonnées de votre cloud. Implémentez une segmentation cohérente et dynamique dans les conteneurs et environnements multicloud.



Confinez les compromissions sur un seul poste de travail, ordinateur portable ou machine virtuelle, avant même que celles-ci soient détectées par d'autres outils de sécurité. Visualisez le trafic des communications des terminaux et des applications au sein de votre réseau et appliquez le principe du moindre privilège.

Confinez les compromissions dans les centres de données locaux, les conteneurs, les environnements IT/OT et les machines virtuelles. Bénéficiez d'une visibilité complète sur tout le trafic, quelle que soit l'architecture, la taille ou la complexité de votre réseau. Segmentez les charges de travail sans interrompre les opérations.

Tirez parti de notre graphe de sécurité optimisé par l'IA

La plateforme Illumio repose sur un graphe de sécurité optimisé par l'IA qui offre une vue inégalée en temps réel de votre surface d'attaque. Illumio Insights et Illuminio Segmentation fonctionnent conjointement pour vous offrir une plateforme complète de confinement des compromissions.

Illumio Insights offre une solution cloud de détection et réponse (CDR) optimisée par l'IA qui identifie les risques, détecte les attaques et confine les menaces de façon instantanée, à l'échelle du cloud. Illuminio Segmentation vous aide à visualiser rapidement les risques et à appliquer des stratégies pour éviter la propagation des compromissions.

Confinez les compromissions avec Illumio Segmentation

illumio.com/fr/illumio-segmentation

À propos d'Illumio

Leader du confinement de ransomwares et de compromissions, Illumio redéfinit la façon dont les entreprises bloquent les cyberattaques et renforcent la résilience opérationnelle. Optimisée par un graphe de sécurité basé sur l'IA, notre plateforme de confinement des compromissions identifie et confine les menaces dans les environnements multicloud hybrides pour empêcher la propagation des menaces avant qu'elles ne donnent lieu à des incidents majeurs.

Classé parmi les leaders du rapport Forrester Wave™ sur les solutions de microsegmentation, Illumio favorise l'implémentation du modèle Zero Trust et renforce ainsi la cyberrésilience de l'infrastructure, des systèmes et des entreprises qui font tourner le monde.