illumio

BRIEF SECTORIEL

Illumio : Protéger le secteur bancaire

Les banques et autres institutions financières se tournent vers la segmentation Zero Trust pour se protéger contre les rançongiciels et les violations

Pourquoi le secteur est-il en danger ?

Les banques, les maisons d'investissement, les courtiers de vente au détail, les prêteurs, les start-up fintech et autres institutions de services financiers sont du « gros gibier » pour les cybercriminels. La raison est simple : C'est là qu'est l'argent.

Selon un rapport d'IBM, les services financiers ont été les principaux secteurs ciblés par les cybercriminels pendant cinq années consécutives, de 2016 à 2020. En 2021, les services financiers représentaient 22,4 % des attaques, en deuxième position derrière l'industrie manufacturière, mais ils restaient une cible privilégiée pour les rançongiciels et autres cyberattaques.

Parmi les types d'attaques, les rançongiciels étaient de loin les plus répandus dans les services financiers, représentant 36 % des attaques dans tous les secteurs, selon IBM.

Le risque de violation de la sécurité s'accroit à mesure que les banques et autres institutions subissent une transformation numérique, introduisent de nouveaux systèmes cloud et étendent les partenariats avec des produits et des prestataires de services tiers. Une activité de fusions et acquisitions rapide, l'utilisation continue des systèmes informatiques et de cybersécurité existants et une évolution vers le travail à distance peuvent également éroder la posture sécurité d'une institution.

Ces changements technologiques et commerciaux élargissent la surface d'attaque et posent de nouveaux problèmes de visibilité. La détection et l'identification d'une violation deviennent de plus en plus difficiles sur des réseaux complexes et interconnectés. Si une violation se produit effectivement, une banque peut subir des pertes financières considérables et une publicité négative susceptibles de saper la confiance des clients commerciaux et de détail, des partenaires commerciaux, des contreparties, des investisseurs et des régulateurs.

Se protéger contre les rançongiciels et autres types de violations est désormais plus qu'un simple problème de cybersécurité : c'est un défi lancé à la résilience de l'entreprise aux niveaux les plus élevés.

Comment Illumio peut aider

Protéger les données des clients

Connaître l'accès aux systèmes, mettre en œuvre des politiques de sécurité pour limiter l'accès, et signaler et analyser tout trafic qui ne correspond pas aux règles.

Atteindre la conformité réglementaire

Délimiter les vulnérabilités dans l'ensemble de l'environnement, cartographier les dépendances des applications, appliquer des politiques granulaires de segmentation et surveiller la connectivité au niveau des violations de conformité.

Activer la transformation numérique

Utiliser la visibilité dans les relations entre les centres de données et les composants du cloud, pour sécuriser les applications sur site et dans le cloud de manière cohérente, et intégrer les processus DevOps pour automatiser la sécurité à grande échelle.

« Avec Illumio, nous avons fait un progrès important pour maximiser la sécurité et minimiser le risque de perturbations opérationnelles ».

Steffen Nagel
Responsable informatique
Frankfurter Volksbank

Appliquer la segmentation Zero Trust à la banque

La technologie de segmentation Zero Trust d'Illumio améliore les défenses traditionnelles par périmètre et pare-feu pour intégrer la sécurité à un niveau beaucoup plus granulaire à l'intérieur des réseaux et des centres de données. Au lieu d'un pare-feu unique protégeant des centaines d'applications et d'appareils, la sécurité est appliquée à chaque ressource individuellement.

Illumio suit le principe Zero Trust selon lequel aucune application, aucun appareil ou utilisateur ne peut être fiable sans vérification et ne peut donc avoir que l'accès le moins privilégié. Par conséquent, les institutions financières peuvent protéger les ressources essentielles et empêcher les acteurs malveillants d'atteindre les systèmes et données critiques, empêchant ainsi une perte de données clients et de marché, ou une défaillance opérationnelle majeure.

Les capacités fondamentales d'Illumio permettent aux banques et autres institutions financières de :

- Sécuriser les ressources et services critiques, même en cas de violation.
- Arrêter la propagation des rançongiciels dans les réseaux, les serveurs des centres de données et les applications.
- Bénéficier d'une visibilité complète sur les applications, les appareils et les réseaux.

Sécuriser les ressources et services critiques

La segmentation Zero Trust d'Illumio fait en sorte que l'accès à toute ressource ou application est sécurisée et authentifiée. Elle élimine les chemins qui permettent un mouvement latéral et applique et maintient la politique dans de grands environnements en évolution rapide.

- Segmenter facilement les ressources, les environnements, les utilisateurs et les groupes.
- Appliquer des politiques de manière dynamique pour sécuriser systématiquement les applications, les appareils et les réseaux en constante évolution.

Arrêter la propagation des rançongiciels

Illumio réduit immédiatement votre surface d'attaque en automatisant les flux de travail (tels que la découverte, la création, la distribution et la mise en application des politiques), qui bloquent les communications sur n'importe quel port à haut risque de votre réseau, ce qui restreint les vecteurs couramment mis à profit par les rançongiciels.

- Identifier vos principales sources de risque en matière de rançongiciel.
- Fermer et surveiller de manière proactive les chemins à haut risque.
- Créer un commutateur de confinement réactif pour arrêter les incidents en cours.

Obtenir une visibilité complète

Illumio fournit des informations exploitables en cartographiant toutes les communications entre les ressources, y compris les applications, les clouds, les conteneurs, les centres de données et les appareils points de terminaison. Et cela sans toucher ni changer votre réseau.

- Partagez une vue unifiée de vos communications pour vos équipes et vos outils SIEM/SOAR.
- Réduire le risque opérationnel en identifiant les connexions inutiles.

Illumio permet aux banques d'empêcher les rançongiciels et les violations de provoquer une défaillance majeure de l'entreprise en protégeant les applications critiques.

Améliorer la cyber-résilience

Découvrez comment Illumio aide le secteur bancaire à protéger les systèmes critiques.

illumio.com/solutions/banking-and-financial-services

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.