illumio

MIEL

Livre Blanc

Comment éviter qu'une attaque par ransomware ne devienne un véritable désastre !

Les étapes essentielles pour réduire le risque que présentent les ransomwares avec la segmentation Zero Trust.

Traduit de l'anglais « How to Prevent Ransomware From Becoming a Cyber Disaster », Illumio

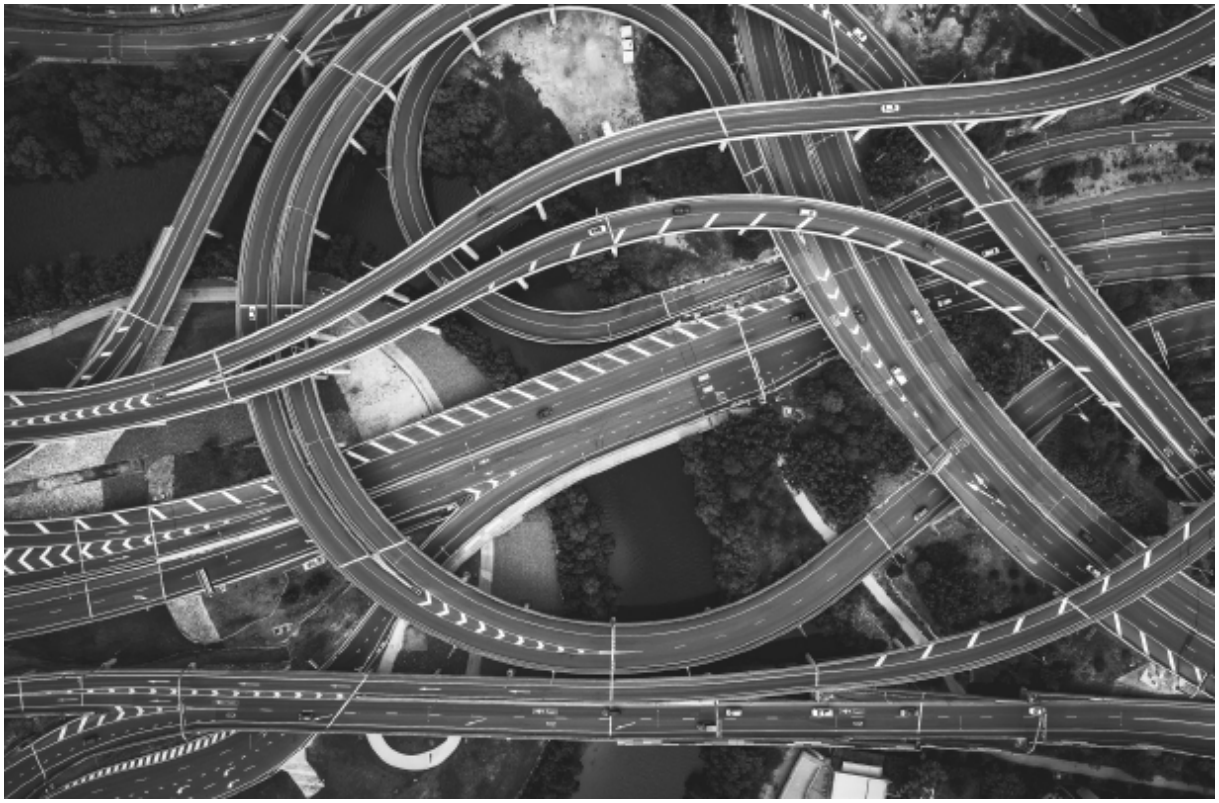


Table des matières

Chaque année et plus particulièrement depuis l'an dernier, les ransomwares constituent l'une des plus grandes menaces de cybersécurité. Chaque semaine, nous apprenons qu'une entreprise d'importance stratégique a été victime d'une intrusion, a payé une rançon ou a vu ses revenus et ses clients menacés. Rappelez-vous, environ 40 % de la population des États-Unis a eu des difficultés à trouver de l'essence après qu'une attaque par ransomware ait touché le principal fournisseur de la côte Est[1]. À la suite de cette attaque, le Président des États-Unis a imposé de nouvelles mesures de sécurité[2] au gouvernement américain et, dans une directive distincte, a recommandé à toutes les entreprises d'adopter une approche de cybersécurité Zero Trust comme seule solution pour se défendre contre les ransomwares. Ces mesures sans précédent montrent à quel point cela perturbe nos vies et l'économie en général.

Le coût d'une brèche monte en flèche

Les ransomwares modernes/nouvelle génération présentent plusieurs caractéristiques clés qui rendent la résolution d'une attaque très difficile :

- Voler les identifiants administratifs des systèmes
- Crypter autant que possible le contenu, le rendant ainsi inutilisable.
- Détruire les sauvegardes, de sorte que la restauration soit impossible sans payer.
- Exposer publiquement les victimes afin d'intensifier la pression pour qu'elles paient.
- Faire fuiter les données volées, ce qui peut entraîner une violation des contrats ou compromettre la compétitivité des entreprises ciblées.
- Menacer les clients de la victime afin d'augmenter la pression et qu'elle paie plus rapidement.
- Poser des ultimatums pour accélérer le versement de rançon : "…avant que le prix n'augmente".

Ces caractéristiques rendent la gestion des attaques par ransomware beaucoup plus couteuse que jamais. La plupart des entreprises de petites tailles paient la rançon puis doivent faire face à des coûts de nettoyage et de remédiation, sans parler de la perte de revenus et du retard pris sur les autres projets. La plupart des analystes s'attendent à ce que les coûts liés aux ransomwares augmentent considérablement à mesure que le « *business model* » évolue. À l'échelle mondiale, les rapports estiment que les coûts de remédiation dépasseront 20 milliards de dollars américains en 2021[3].

[1] Source : https://www.nbcnews.com/politics/national-security/russian-criminal-group-may-be-responsible-colonial-pipeline-ransomware-attack-n1266793

[2] Source : https://fortune.com/2021/05/14/biden-white-house-cybersecurity-order-ransomware-zero-trust/

[3] Source : https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Le modèle de sécurité standard n'aide pas beaucoup

Malheureusement, l'architecture de sécurité que nous nous sommes efforcés de construire pendant les 15 dernières années n'arrête guère les ransomwares, et dans de nombreux cas, elle leur permet même de faire facilement leur sale boulot !

L'idée d'un périmètre consolidé, avec ses analogies aux murs des châteaux médiévaux et aux contrôles physiques, offre un attrait indéniable. Après tout, nous plaçons des serrures et des agents de sécurité devant les bâtiments pour en contrôler l'accès. Mais, tout comme la plupart des sites qui offrent un libre accès une fois passé le bureau d'accueil, sans autre vérification d'identité pour parcourir les couloirs, l'intérieur du S.I. est vulnérable. Une fois passé le périmètre de sécurité ou les suites de sécurité des ordinateurs portables, le réseau vous emmène où vous voulez. Et les ransomwares s'introduisent donc partout et immédiatement via le réseau. La plupart des ransomwares peuvent infecter un réseau entier en quelques secondes, en passant facilement d'une machine à l'autre via les ports qui sont activés par défaut sur la majorité des machines.

Bien sûr, nous avons augmenté la sécurité périmétrique au fil des ans avec des scanners, des outils d'analyse, du *Machine Learning*, des outils prédictifs et diverses technologies pour sécuriser les *endpoints*. Et pourtant, l'actualité prouve que nous n'avons toujours pas réussi à stopper les attaques par ransomware. De nombreuses entreprises souffrent en silence.

En 2021, le coût des remédiation des attaques par ransomwares est estimée à 20B$

Pourquoi les attaques passent-elles les barrières de sécurité ?

Dans de nombreuses entreprises, le périmètre s'est effectivement dissous avec les ordinateurs portables individuels, ce qui crée de nombreux nouveaux problèmes. La plupart des entreprises ont des collaborateurs qui travaillent à distance, depuis leur domicile ou sur des sites distants. En dehors des logiciels qu'on peut installer à distance, plus rien de ne relie les appareils des utilisateurs au périmètre.

Et ce ne sont pas uniquement les utilisateurs qui si sont déplacé hors du *data center.* Les applications sont désormais constituées comme des services distribués. Certaines ont évolué vers des conteneurs générés dynamiquement à la demande. D'autres services applicatifs proviennent de solutions SaaS ou hébergées dans le cloud. La plupart des entreprises ont une stratégie multicloud par défaut. Les licences Microsoft d'entreprise imposent habilement l'utilisation d'Azure ou des services cloud de Microsoft, et Amazon est un emplacement par défaut pour nombre de services cloud. Ainsi, lorsqu'un utilisateur clique sur un faux lien et se retrouve infecté malgré lui, il suffit d'une simple faiblesse dans l'environnement cloud des applications distribuées pour que l'attaque se propage d'un environnement à l'autre. Dans de trop nombreux cas, cela se produit en quelques secondes -bien plus rapidement que les capacités de réponse de la plupart des outils de détection.

Protection des services critiques, des environnements de calcul et des *endpoints*.

Les contrôles les plus importants pour lutter contre les ransomwares sont ceux qui sont en place avant toute infection. La plupart des RSSI s'accordent à dire que la formation des utilisateurs finaux a ses limites. Plus il y a de collaborateurs dans l'entreprises, plus le risque de compromission est élevé.

En conséquence, de nombreuses entreprises ont adopté une posture « *assume breach* » (« brèches assumée ») ou ont commencé à employer des termes comme « sécurité post-intrusion ».

Après tout, même si un poste est infecté, il a toujours besoin d'une route pour se propager et transmettre son code malveillant à un autre utilisateur ou à un serveur. Lorsque ces routes ne sont pas accessibles et que des alarmes sont déclenchées à cause d'une violation des politiques de sécurité, les outils et les équipes de détection en place disposent des quelques secondes, minutes ou heures critiques dont ils ont besoin pour identifier et mettre en quarantaine la menace.

Les brèches sont probablement inévitables mais une infection totale du système l'est !

L'attention du marché se tourne vers une approche dite « *Zero Trust* » afin de renforcer les contrôles sur les réseaux, les utilisateurs, les données, les *devices* en utilisant le principe du "moindre privilège". Ce principe, qui remonte au début des années 1970, consiste à affirmer que l'accès aux réseaux, aux systèmes, aux comptes ou aux données devrait être limité au minimum nécessaire. Le principe du *Zero Trust* garantit que seuls les trafics autorisés sont permis. Le président des États-Unis a d'ailleurs récemment imposé une architecture *Zero Trust* pour la plupart des agences gouvernementales américaines et l'a recommandée pour toutes les entreprises.

La segmentation Zero Trust élimine 90 à 99% des chemins de connexion.

Si on applique cela au réseau, les anciens réseaux largement ouverts se transforment en zones fortement cloisonnées où les mouvements dans le data center, le cloud ou entre les conteneurs sont limités. La segmentation *Zero Trust* réduit les connexions au strict nécessaire et élimine généralement 90 à 99 % des chemins de connexion dans le data center. Lorsqu'elle est mise en œuvre dans un modèle distribué où chaque serveur, instance de système d'exploitation et conteneur devient un point d'exécution, chaque serveur devient un capteur. Toute violation de la politique de sécurité ou toute recherche de ports ouverts déclenche immédiatement une alerte, même si l'accès est refusé.

Il s'avère que la plupart des ransomwares suivent le chemin de la moindre résistance. Et plus de 70 % des attaques des ransomwares utilisent des protocoles courants comme le protocole RDP (*Remote*

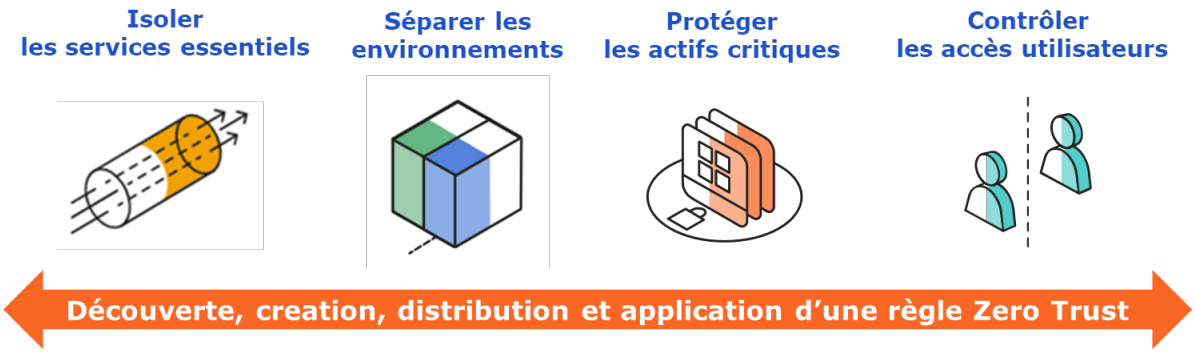
Desktop Protocol) ou des technologies de partage de fichiers comme le SMB (Server Message Block). Ces protocoles sont "activés par défaut" dans les installations standards des systèmes d'exploitation. Mais, fait intéressant, la plupart des utilisateurs n'utilisent ni l'un ni l'autre.

Alors, pourquoi ces ports sont-ils ouverts ?

Selon les principes de la segmentation *Zero Trust*, les ports inutilisés ne doivent ni envoyer, ni recevoir de données. Si vous éliminez l'accès permettant à l'infection de se propager, elle ne pourra tout simplement pas le faire. En réduisant les ports ouverts au strict nécessaire, il n'existera que très peu de voies de sortie depuis un poste infecté, et la plupart ne sera pas vulnérable aux tentatives d'*exploits* des attaquants. Cela donne un indice du meilleur endroit où commencer à réduire le risque de ransomware.

Un moyen rapide de réduire le risque lié aux ransomwares

Le moyen le plus rapide de réduire le risque de propagation des ransomwares avant qu'une infection ne se produise est de supprimer les chemins d'accès qu'ils utilisent pour se propager. À partir de là, des contrôles supplémentaires peuvent être mis en place pour s'assurer que les autres types d'attaques échouent également.



Les services applicatifs de base se connectent généralement à chaque ordinateur ou instance de serveur. Les applications d'Active Directory, de surveillance, de gestion des performances et de sécurité connectent souvent les systèmes à un cerveau central. Il ne serait donc pas surprenant que ces protocoles soient la première cible de la plupart des pirates. Après tout, la compromission d'un protocole largement utilisé ou d'un serveur central ayant accès à toutes les autres machines de l'environnement va accélérer l'infection sur tout le système de l'entreprise.

Mais, si l'on met de côté ces services de base, d'autres formes de segmentation contribuent à restreindre les activités malveillantes quel qu'en soit le type. Cloisonner logiquement les systèmes et les utilisateurs en fonction de leur rôle, de leur environnement et de leur emplacement, permet de réduire le nombre de connexions possibles. Toutefois, s'il existe, par exemple, de nombreux systèmes dans ces regroupements, il peut être judicieux d'affiner encore la segmentation afin que les applications soient vraiment isolées et cloisonnées les unes par rapport aux autres. Si une application

est compromise mais ne peut communiquer avec aucune autre, le potentiel de propagation est radicalement réduit.

Et avec la bonne technologie de segmentation, il est même possible d'appliquer le principe du *« Zero Trust »* à chaque flux, éliminant ainsi le risque qu'un trafic non autorisé trouve un port ouvert à exploiter.

Vous voulez réduire rapidement les risques liés aux ransomwares ? Respectez quelques étapes importantes pour y arriver !

Isoler les services de base et d'administration

Vous réduirez le risque dès le moment où vous isolerez les services administratifs et les services de base, avec une utilisation limitée au strict nécessaire.

Pour prendre un exemple simple, un groupe d'administrateurs peut avoir besoin d'utiliser RDP pour administrer des serveurs, mais ce n'est pas le cas des autres utilisateurs. Les serveurs ne doivent ainsi pas accepter de connexions RDP de leur part.

Considérons les ports qui présentent le plus grand risque :

	Exemple	Risque
Ports hautement connectés	Services de base Ports de management Système de Polling / Reporting	Exposition à tout l'environnement
Ports « peer-to-peer »	RDP, WinRM, SMB, RPC, WMI, DCOM, Réseaux sociaux	Un traffic « machine-to-machine" qui serait normal
Applications collaboratives	Base de données Services de base Applications Microsoft Utilitaires Linux communs	Nombreuses vulnérabilités publiées

- **Les ports hautement connectés** sont les plus efficaces pour propager une infection, tout comme un réseau autoroutier relié à de nombreuses villes est le meilleur moyen de déplacer des marchandises dans un pays. Les services de cœur et d'admin se connectent généralement à la plupart des systèmes d'un environnement informatique. Mais si chaque serveur peut avoir besoin de communiquer via un port avec un système central, aucun serveur ne doit pouvoir communiquer avec un autre serveur sur ce port. Il suffit donc de fermer les ports à destination de tout host non légitime pour éliminer la propagation latérale d'un service.

- **Les protocoles peer-to-peer** visent à permettre à toute machine de contacter une autre machine d'une manière bien définie dans le but d'échanger simplement des données. Cela pourrait donc sembler être une cible idéale pour y introduire un code malveillant ou un ransomware. Si chaque serveur ou ordinateur portable s'attend à discuter avec n'importe quel autre serveur, alors n'importe quel serveur peut infecter tous les autres – ce qui serait la pire des situations.
  Si le trafic *"n'importe où vers n'importe où"* est normal, comment détecter les anomalies ? Là encore, ces protocoles devraient être fortement limités.
  De nombreuses entreprises exigent des administrateurs qu'ils se connectent d'abord à un système sécurisé - un "jump box" - et qu'ils l'utilisent ensuite comme seule source acceptable pour les connexions de bureau à distance. Lorsqu'il est renforcé par une segmentation *Zero Trust*, un protocole *peer-to-peer* largement ouvert se limite à un seul système, ce qui réduit radicalement le potentiel de propagation latérale.

- **Les ports les plus connus** ont à la fois l'avantage et l'inconvénient d'être largement utilisés. Comme ces ports existent depuis de nombreuses années, voire des décennies, ils peuvent constituer un moyen fiable d'échanger des informations. Mais cette longévité signifie également que les acteurs malveillants ont eu des années pour les étudier et trouver des vulnérabilités et des *exploits*. Étant donné qu'aucun correctif n'élimine les anciens logiciels, les pirates peuvent jouer la carte de la chance et ils trouvent généralement un système vulnérable aux attaques. Lorsque la segmentation *Zero Trust* ferme ces ports ou les limites à des flux spécifiques et intentionnels, il n'est plus possible pour un acteur malveillant de s'en servir.

La réduction combinée des possibilités de connexion pour les ports fortement utilisés, les protocoles *peer-to-peer* et les ports usuels minimise radicalement le potentiel de propagation des logiciels malveillants. La plupart des attaques utilisent des vulnérabilités connues et des ports connus pour se déplacer, et la segmentation *Zero Trust* élimine ces chemins d'accès sans interrompre le trafic applicatif existant. Comme ces ports sont courants et ne concernent généralement qu'une poignée de destinations autorisées dans le *data center*, l'élaboration de la politique de segmentation est rapide. Très souvent, quelques minutes suffisent pour mettre en place une politique de *Zero Trust.*

Renforcer le contrôle des environnements

Après avoir pris le contrôle sur les services de base et de gestion, le renforcement des contrôles des environnements devrait être la prochaine étape. La plupart des entreprises font déjà une certaine distinction entre les environnements de développement, de test et de production. Mais au-delà du renforcement de ces contrôles, il est souvent possible d'identifier des restrictions additionnelles faciles à mettre en place et de renforcer les contrôles IT/OT.

Au-delà d'un simple pare-feu entre les environnements de DEV (Développement) et PROD (Production), la plupart des entreprises pourraient renforcer considérablement leurs contrôles. Au fil du temps, les règles de sécurité mises en place initialement dérivent, et souvent pour gérer un cas d'usage particulier, certaines règles sont assouplies, puis oubliées ou non restreintes par la suite. Par exemple, l'équipe informatique étant l'utilisateur principal de l'environnement DEV et l'administrateur système celui de l'environnement PROD, il est fréquent que l'accès soit ouvert aux deux pour des raisons de facilité d'utilisation.

En mettant en place une solution de segmentation *Zero Trust* efficace, tous les flux DEV-vers-PROD vont rapidement être cartographiés et classifiés pour analyse. Au lieu d'essayer de faire correspondre ces flux particuliers a des règles générales de firewall, il devient plus facile de visualiser et d'identifier les flux vraiment légitimes, puis de simplement bloquer tout le reste. Eliminer les routes non nécessaires va non seulement épurer les accès administratifs, mais aussi réduire la possibilité de propagation d'une infection d'un environnement à un autre.

Il est souvent possible d'identifier des restrictions faciles à mettre en place et de renforcer les contrôles IT/OT

Mais même en se limitant à l'environnement de PROD ou à une portion d'un déploiement cloud, on pourrait identifier à l'intérieur des frontières simples à mettre en place. Il y a par exemple du trafic de bases de données derrière la plupart des applications, et ce trafic se limite généralement à un port ou un groupe de port. Contrôler l'accès des données et l'accès admin aux clusters de données serait ainsi simple et rapide, et permettrait de protéger un des actifs les plus critiques de l'entreprise.

On pourrait en faire de même pour les applications « bijoux de la couronne », les plus précieuses, pour lesquelles les schémas de communications peuvent être larges mais bien définis. Sans forcément beaucoup de détail, il est possible d'isoler ces applications d'une grande partie du reste du data center.

De même, renforcer les contrôles autours des systèmes OT et des systèmes intégrés en général ne doit pas présenter plus de difficultés. Il y a beaucoup de systèmes intégrés dans un data center – concentrateurs VPN, Baies de stockage, et toute autre type d'appliances. Limiter ces appareils aux seuls ports nécessaires, et restreindre les machines clientes à seulement écouter l'appliance, réduit significativement leur exposition. Les caméras IP, les lecteurs de badge, les imprimantes et tout le monde des systèmes OT devraient être positionné derrière une frontière à travers laquelle ils ne pourraient communiquer qu'avec leur serveur de contrôle sans lien possible avec le reste du data center.

Contrôler la connectivité des terminaux pour limiter les infections

Si le *data center* est la cible ultime de la plupart des ransomwares, les infections s'installent généralement d'abord sur les *endpoints* des utilisateurs.

Il existe plusieurs stratégies clés pour réduire, dès le départ, le risque de propagation des ransomwares :

- **Fermez tous les ports inutilisés**
  Les systèmes d'exploitation des ordinateurs ont généralement un profil très ouvert. Pourtant, la plupart des collaborateurs utilisent un ensemble très restreint d'applications et de services. La fermeture des ports inutilisés les élimine comme vecteur potentiel de propagation.

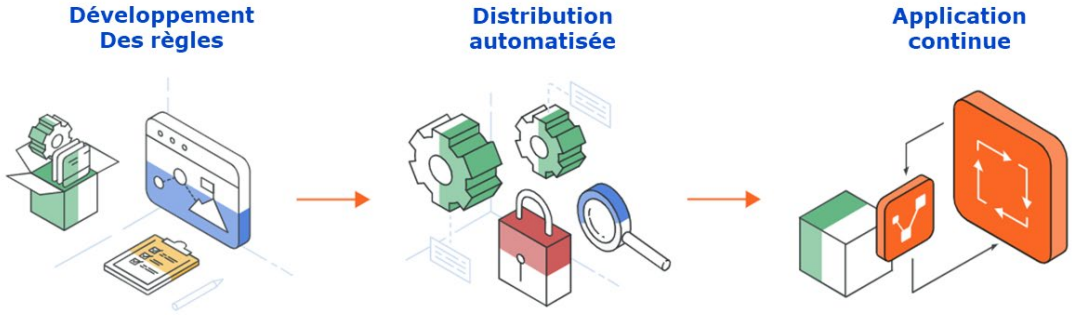
- **Éliminez la propagation *Peer-to-Peer***
  Le contrôle des protocoles *poste-à-poste* aux extrémités du réseau élimine de nombreuses stratégies courantes de propagation des ransomwares. RDP, SMB et autres protocoles similaires peuvent être également bloqués en entrée et en sortie.

- **Contrôler l'accès aux actifs du cloud et du data center**
  Comme à l'intérieur du data center, une fois que les services de base sont sécurisés et que les ports inutilement ouverts sont fermés, l'étape logique suivante consiste à s'assurer que les utilisateurs ne peuvent envoyer et recevoir du trafic que vers les serveurs autorisés et inversement que les serveurs n'acceptent que le trafic des utilisateurs autorisés. La segmentation *Zero Trust* peut coordonner les politiques de sécurité entre les *endpoints* et les serveurs pour s'assurer que ces règles soient appliquées partout.

- **Lier les politiques de *Zero Trust* à l'identité**
  L'identité de l'utilisateur constitue la meilleure base pour contrôler l'accès de cet utilisateur au *data center* ou au cloud. Avant la connexion, il n'y a aucune raison pour que les serveurs et les applications soient ouverts à un ordinateur donné. Lors de la connexion, l'accès peut être ouvert uniquement aux ressources nécessaires. Lorsque l'utilisateur se déconnecte, les autorisations d'accès peuvent être révoquées. Contrairement à l'approche par défaut "*always on, always open*", la segmentation basée sur l'identité garantit que les ports ne sont ouverts que lorsque cela est nécessaire.

Automatisation et Evolution de la protection *Zero Trust*

Les ransomwares ne dorment jamais ! Et votre infrastructure *Zero Trust* doit en faire autant ! L'automatisation des politiques de sécurité permet une application continue des règles définies. Une fois qu'une entreprise a élaboré une politique pour certains ou tous les scénarios mentionnés ci-dessus, cette politique doit être distribuée dans l'environnement à chaque serveur, machine virtuelle, *endpoint*, conteneur et système cloud. L'automatisation peut garantir que tous les systèmes appliquent en permanence la politique de sécurité définie, même lorsque les adresses IP changent, que de nouvelles instances d'applications sont installées ou qu'elles sont supprimées.



Capacités clés d'une solution de segmentation efficace pour assurer automatisation et évolutivité

Intégrer une politique Zero Trust dans chaque Workload
Une bonne segmentation Zero Tru*st* doit pouvoir accompagner le serveur / conteneur tout au long son cycle de vie. Il faut pouvoir mettre en place cette stratégie *Zero Trust* dès la définition des modèles (ou image de référence) afin que l'ensemble des images cibles prennent nativement en compte cette politique. La gestion des mises à jour de cette segmentation *Zero Trust* doit pouvoir ensuite être apportée dynamiquement via des processus d'automatisation à l'ensemble des environnements, même les plus volatiles, pour pouvoir se conformer aux stratégies à tout moment.

Fournir une "Segmentation as a Service" au DevOps
Les moteurs de règle de segmentation *Zero Trust* offrent généralement un accès API complet et une abstraction totale de l'infrastructure sous-jacente. Cela signifie que la segmentation fonctionne comme n'importe quel autre service d'application cloud. Le code DevOps peut instancier des systèmes, demander des services de segmentation et se conformer instantanément aux règles de sécurité en place, le tout en quelques secondes. Lorsque la segmentation *Zero Trust* n'est qu'un simple service comme les autres, la barrière à l'adoption tombe et la posture globale de sécurité de l'entreprise s'améliore.

Réduire les efforts d'administration
Les *ransomwares* se déplacent beaucoup trop rapidement pour que les règles des *firewalls,* ajustées manuellement, aient un quelconque effet. La politique de segmentation *Zero Trust* doit être constamment et continuellement mise à jour. Une politique de sécurité Zero Trust automatisée évite les interventions manuelles fastidieuses liées à une politique traditionnelle de pare-feu, et devient ainsi beaucoup plus facile à administrer.

Éliminer la dépendance au réseau et les process manuels
L'automatisation ne peut fonctionner que si les objets automatisés sont décorrélés de

l'infrastructure physique. Lorsque la segmentation fait abstraction de l'architecture réseau, elle peut être complètement automatisée à l'instar des VM et du « server build ».

La segmentation *Zero Trust* utilises des labels provenant d'informations déjà exploitées par l'entreprise, et pourrait donc être rapidement reliée à une automatisation qui serait déjà présente. De plus, comme elle utilise les firewalls déjà embarqués dans les systèmes d'exploitation ou les conteneurs, il n'y a aucune dépendance vis-à-vis de l'architecture réseau ou de la technologie. On peut donc mettre en place une règle arbitraire de segmentation sans jamais avoir à changer un matériel réseau ou sa configuration

Être confiant face aux menaces

Il est facile d'imaginer toutes sortes de stratégies multipliant les produits de sécurité pour combattre les différents aspects d'une attaque par ransomware. Mais en se concentrant sur les éléments fondamentaux, on obtient de meilleurs résultats : les logiciels malveillants ne peuvent pas se propager là où ils ne trouvent pas d'accès au réseau.

Il n'est pas nécessaire de consacrer beaucoup de temps et d'efforts pour obtenir les résultats suivants :

Parmi les succès obtenus grâce à la segmentation *Zero Trust*, citons :

- 11 000 systèmes basculés vers une politique *Zero Trust* en trois mois pour réussir un audit
- 40 000 systèmes sécurisés dans le cadre d'une automatisation DevOps complète
- Isoler 1 trillion de dollars par jour de transactions financières dans une seule banque
- Sécurisation des données personnelles de chaque titulaire d'hypothèque aux États-Unis
- 145 000 systèmes sécurisés dans une entreprise mondiale

Les ransomwares représentent l'une des menaces les plus fréquentes auxquelles sont confrontées les équipes IT d'une entreprise. Mais il est possible de prendre des mesures immédiates pour empêcher une infection de faire des dégâts irréversibles.

Aucune entreprise n'est à l'abri qu'un utilisateur clique sur un lien frauduleux, mais lorsque leurs ordinateurs portables sont bien isolés, que les ports principaux et d'admin sont verrouillés et que les contrôles des environnements sont renforcés, les ransomwares ne peuvent tout simplement pas se déplacer dans le *data center*.
Mieux encore, la segmentation « *Zero Trust* » n'est pas seulement efficace contre les ransomwares - elle élimine les mouvements latéraux de toute personne ou logiciel agissant avec une intention malveillante. La segmentation « *Zero Trust* » ne repose pas sur une capacité de détection ou d'analyse. Il s'agit d'un contrôle proactif qui fonctionne en permanence, constamment actif et précis grâce à l'automatisation.

A propos de Illumio

Illumio, pionnier et leader du marché de la segmentation Zero Trust, empêche les brèches de devenir des désastres industriels. Illumio protège les assets et applications critiques grâce à une technologie de segmentation éprouvée et spécialement conçue pour le modèle de sécurité Zero Trust. Ses solutions Illumio Core et Illumio Edge automatisent l'application des règles de sécurité pour éviter que les cyberattaques et les ransomwares ne se propagent à travers les applications, containers, clouds, data centers et endpoints.

A propos de Miel

Créée en 1985, MIEL introduit sur le marché français, via un réseau d'intégrateurs qualifiés, les nouvelles technologies à l'attention des DSI et des Cloud providers dans le domaine de la cybersécurité, des réseaux, du cloud et du *digital workplace*.

Notre valeur ajoutée :
Aider nos intégrateurs partenaires dans les phases de qualification, de maquette, d'implémentation et d'après-vente ; et faire de chaque projet une réussite pour leurs clients.
Rencontrer les directions informatiques et faire la preuve de l'efficacité de nos technologies pour leurs projets de transition numérique sécurisée vers le Cloud et la mobilité.

Miel, distributeur Illumio en France, contactez-nous :

01 60 19 34 52 / reseausecu@miel.fr