

# Rompres la chaîne d'attaque des ransomwares

## Cinq étapes pour bloquer les mouvements latéraux

Les attaques par ransomware ne se propagent pas en infiltrant une seule machine ou un seul terminal. Les cybercriminels utilisent cette souche de logiciels malveillants pour crypter la plus grande partie possible d'un réseau afin de garantir que les victimes paient la rançon.



Toutes les 2 secondes

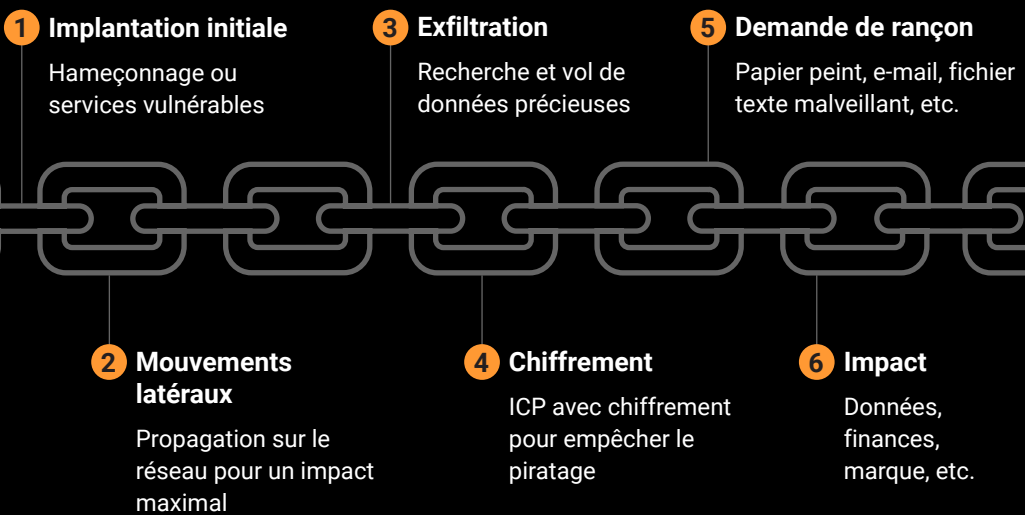
D'ici 2031, les ransomwares devraient attaquer une entreprise, un utilisateur ou un terminal toutes les deux secondes.

[Rapport sur le marché du ransomware de Cybersecurity Ventures](#)

## Avez-vous confiance en votre sécurité réseau actuelle ?

Si vous comptez toujours sur les anciens pare-feu pour la segmentation, vous ne pourrez pas empêcher les ransomwares de se propager sur votre réseau et de vous bloquer l'accès aux applications et infrastructures critiques.

## La chaîne d'attaque des ransomwares



## Les violations sont inévitables

Vous avez besoin d'une solution de sécurité détectant les menaces dans le trafic est-ouest du centre de données et bloquant les mouvements latéraux.

## Rompres la chaîne



**Se préparer** en identifiant chaque application et chaque ressource en cours d'exécution dans votre environnement informatique



**Prévenir** en créant des règles pour bloquer les techniques de propagation de ransomware courantes



**Détecter** en recevant des alertes pour toute tentative d'accès aux applications segmentées et aux sauvegardes



**Résoudre** en lançant des mesures de confinement des menaces et de quarantaine lorsqu'une attaque est détectée



**Récupérer** avec des fonctionnalités de visualisation prenant en charge les stratégies de récupération par phases

En 2022, les attaques par ransomware ont augmenté de près de 13 %, soit une hausse aussi importante que les cinq dernières années combinées.

[Verizon 2022 Data Breach Investigations Report](#)

Si vous n'êtes pas préparé pour vous défendre contre une recrudescence d'attaques et de demandes de rançon plus élevées, il est temps d'intégrer la segmentation et la visibilité à votre stratégie de défense.

[En savoir plus](#)