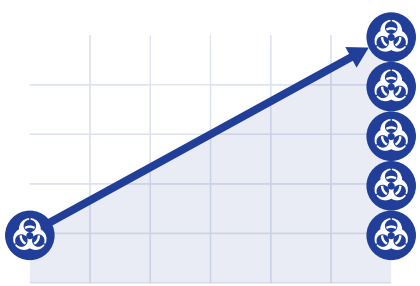
Neutraliser les attaques de Ransomware

Les ransomwares devraient causer **20 milliards de dollars en dommages et intérêts en 2020.** Il est temps d'adopter une nouvelle approche pour empêcher les ransomwares d'avoir un impact sur votre entreprise.

5fois

Plus de ransomwares livrés via SSL au cours des six derniers mois[1]



Décryptez, détectez et empêchez les menaces dans l'ensemble du trafic SSL

Les adversaires contournent les contrôles de sécurité obsolètes en se dissimulant derrière le chiffrement SSL.

Différence d'architecture proxy:

Décryptez et détectez les menaces dans l'ensemble du trafic SSL grâce à l'évolutivité du cloud et une massive capacité de calcul.

[1] Zscaler ThreatLabZ

Mettez en quarantaine les attaques inconnues et neutralisez les programmes malveillants dits patient-zéro

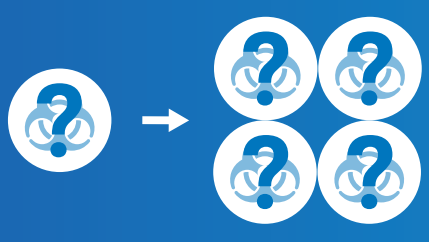
Les hackers viennent à bout des défenses basées sur des signatures en concevant des charges utiles pour chaque cible.

Différence d'architecture proxy:

Arrêtez les attaques de type patient zéro grâce à la quarantaine pilotée par l'IA, laquelle conserve pour analyse les contenus suspects, contrairement aux approches dites passthrough basées sur le pare-feu obsolète.

4x

Plus de variantes de ransomware jamais vus, en 2020[2]



[2] Zscaler ThreatLabZ

38%

Augmentation du trafic à distance[3]

Une sécurité cohérente pour tous les utilisateurs et pour tous les emplacements

Le ransomware ne fait pas de discrimination en fonction de l'emplacement — vous avez besoin d'une sécurité cohérente dans toute l'entreprise.

Différence d'architecture proxy:

Garantir à tous les utilisateurs la même sécurité de haute facture en tout temps, qu'ils soient à la maison, au siège social, ou en déplacement.

[3] Statista

Réduisez instantanément votre surface d'attaque

Les adversaires comptent sur la capacité de pivoter et à se déplacer latéralement sur les réseaux plats désuets pour réussir.

Différence d'architecture proxy:

Opter pour une position zero trust, où il n'existe pas de mouvement lateral. Les applications sont invisibles aux hackers, et les utilisateurs autorisés accèdent directement aux ressources nécessaires, et non à l'ensemble du réseau.

60%

Supprimeront progressivement les VPN au profit de ZTNA (Zero Trust Network Access) d'ici 2023[4]

[4] Gartner Market Guide for Zero Trust Network Access

Neutraliser les ransomwares dès qu'ils surviennent

Passez à une approche fondamentalement différente dans l'enraiement de ransomware avec **Zscaler Zero Trust Exchange™**.

En savoir plus aujourd'hui

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.com