INFOGRAPHIE

Zero Trust : La protection ultime contre les ransomwares

Les attaques de ransomwares, en constante évolution, contournent la sécurité traditionnelle des réseaux.

Alors que les utilisateurs, les applications et les données se sont affranchis du périmètre au cours des deux dernières années, la portée et l'impact des ransomwares se sont accélérés. Les hackers individuels ont été supplantés par des groupes qui s'achètent et se vendent entre eux leurs compétences spécialisées et leurs boîtes à outils. Les attaques, autrefois larges et unidimensionnelles, utilisent désormais des tactiques ciblées et multicouches qu'il est pratiquement impossible d'arrêter avec les architectures de sécurité traditionnelles cloisonnées.

20 Md$
de dommages estimés dus aux ransomwares en 2020

Toutes les 14 secondes
une attaque par ransomware se produit dans le monde entier

500 %
d'augmentation des ransomwares dissimulés dans le SSL pour contourner les défenses traditionnelles

Les ransomwares représentent le plus grand risque pour les entreprises digitales :

Compromission initiale	Mouvement latéral	Données exfiltrées pour une double-extorsion	Introduit une rançon et chiffre les machines	Demande de ransomware
80% des attaques commencent par un e-mail d'hameçonnage	**94 %** des infections mettent moins de 4 heures pour se répandre	**50 %** de toutes les attaques par ransomware sont des failles dans les données	**200 %** d'augmentation des temps d'arrêt dus aux ransomwares	**234 K$** de paiement moyen par ransomware

architecture Zero trust

Reconnaissance → E-mail d'hameçonnage → Macro Malveillante → Installer Malware → Contrôleur de domaine propre → Pirater Identifiants → Déplacer Latéralement → Pirater Données → Installer Ransomware → Demander Rançon

Empêcher l'intrusion

Prévention des attaques grâce à une protection alimentée par l'IA.

Suppression de la surface d'attaque.
Les applications sont invisibles sur Internet et ne peuvent être ni découvertes ni attaquées.

Inspection complète du contenu.
Interruption de chaque connexion pour une inspection en ligne complète de tout le trafic, y compris SSL à l'échelle, avec une architecture de proxy.

Protection des ressources du cloud public.
Correction des erreurs de configuration pour empêcher tout accès non autorisé aux ressources cloud.

Empêcher le mouvement latéral

Blocage des mouvements latéraux grâce à une politique de Zero Trust complète.

Segmentation utilisateur-application.
Connexion directe de l'utilisateur autorisé à la bonne ressource, sans jamais passer par le réseau, grâce à de véritables contrôles d'accès réseau Zero Trust.

Segmentation entre charges de travail.
Extension de l'accès Zero Trust aux communications entre charges de travail pour les environnements hybrides et multi-clouds.

Détection des hackers les plus sophistiqués grâce à la tromperie.
Identification et blocage rapides des hackers les plus avancés grâce à des leurres et des appâts placés dans l'ensemble de l'entreprise.

Empêcher la perte de données

Prevent data theft with complete data loss protection

Prévention du vol de données grâce à une protection complète contre les pertes de données.
Inspection de tout le contenu pour détecter les pertes de données.

Identification et classification des données sensibles.
La correspondance exacte avancée des données et l'empreinte digitale des documents garantissent que les données les plus critiques sont localisées et protégées.

Sécurisation des données SaaS.
Prévention du surpartage et découverte des données sensibles au repos grâce aux meilleures capacités CASB intégrées de leur catégorie

Zero Trust : la stratégie la plus efficace de protection contre les ransomwares

Protection supérieure contre les ransomwares :
L'inspection inline de l'ensemble du trafic pour les entreprises mobiles et cloud first d'aujourd'hui, réduit la surface d'attaque et élimine les mouvements latéraux.

Dépasse les solutions traditionnelles :
Zero Trust propose une approche totalement différente des architectures de sécurité réseau cloisonnées traditionnelles en connectant directement les utilisateurs aux applications, jamais au réseau.

Une sécurité au service de l'entreprise :
Réduit la complexité et les coûts grâce à un modèle de sécurité entièrement délivré dans le cloud, qui supprime l'infrastructure traditionnelle et renforce l'agilité de l'entreprise et l'expérience utilisateur.

Conséquences de l'adoption de Zero Trust pour l'entreprise et la sécurité

Réduction inégalée des risques
Élimine la surface d'attaque et les mouvements latéraux avec une protection supérieure contre les cybermenaces et des données.

35 fois
machines infectées en moins

NOV

Délai de rentabilisation plus court.
Déployé en tant que véritables services cloud avec zéro infrastructure, opérationnel en moins de 24 heures.

Déploiement de
plus de 10 000 utilisateurs
en moins de 48 heures

NORDSTROM

Valeur ajoutée
Supprime les produits de sécurité ponctuels et simplifie les opérations

70%
de réduction des coûts

SIEMENS

Vous souhaitez en savoir plus sur la manière de protéger votre entreprise avec la protection contre les ransomwares la plus complète du marché ? **Téléchargez l'e-book.**

Lire le livre électronique →

Source : https://www.unitrends.com/solutions/ransomware-education

zscaler™