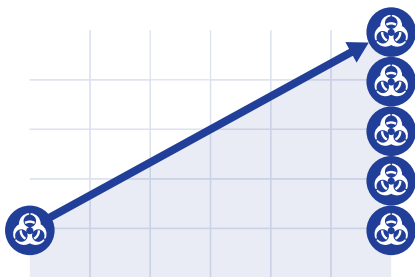


Segreti per fermare i ransomware

Si prevede che i ransomware causeranno **20 miliardi di dollari di danni nel 2020**. È giunto il momento di adottare un nuovo approccio che impedisca a questo tipo di attacchi di colpire le organizzazioni.

5x Crescita dei ransomware erogati sull'SSL negli ultimi sei mesi¹



Decrittografare, rilevare e prevenire le minacce in tutto il traffico SSL

Gli avversari bypassano i controlli di sicurezza legacy nascondendosi nella crittografia SSL.

Differenza dell'architettura proxy:

Decrittografare e rilevare le minacce in tutto il traffico SSL grazie alla scalabilità del cloud e alla massiccia capacità di calcolo.

¹ Zscaler ThreatLabZ

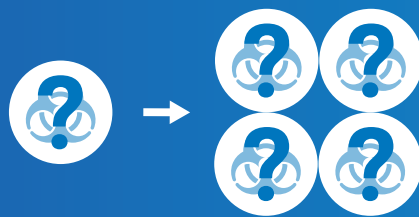
Messa in quarantena degli attacchi sconosciuti e arresto di malware da paziente zero

Gli aggressori superano le difese basate sulla firma, creando carichi utili unici per ogni obiettivo.

Differenza dell'architettura proxy:

Blocca gli attacchi da paziente zero mediante quarantena basata sull'IA, che confina i contenuti sospetti per l'analisi, a differenza degli approcci passthrough basati su firewall legacy.

4x Aumento nel 2020 delle varianti di ransomware mai viste prima²



² Zscaler ThreatLabZ

38% Aumento del traffico remoto³



Sicurezza uniforme per tutti gli utenti e tutte le posizioni

I ransomware non discriminano in base alla posizione: è necessaria una sicurezza uniforme per tutta l'azienda.

Differenza dell'architettura proxy:

Assicura che tutti gli utenti godano sempre della stessa sicurezza sia che siano a casa, in sede centrale o in movimento.

³ Statista

Riduce istantaneamente la superficie d'attacco

Per avere successo gli avversari si affidano alla capacità di districarsi e di muoversi lateralmente attraverso reti flat legacy.

Differenza dell'architettura proxy:

Parte da una posizione Zero Trust dove il movimento laterale non può esistere. Le app sono invisibili agli aggressori e gli utenti autorizzati accedono direttamente alle risorse necessarie, non all'intera rete.

60% Le VPN saranno gradualmente surclassate a favore dello ZTNA (Zero Trust Network Access) entro il 2023⁴



⁴ Gartner Market Guide for Zero Trust Network Access

Previene i ransomware prima che attacchino

Passa a un approccio completamente diverso per fermare i ransomware grazie a **Zscaler Zero Trust Exchange™**.

[Scopri di più oggi](#)