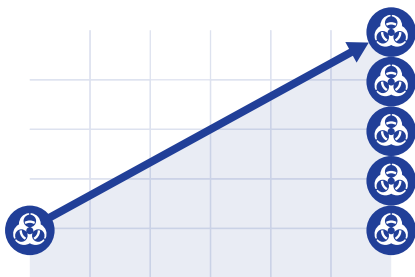


# Secretos para detener el ransomware

Se espera que el ransomware cause **20 mil millones de dólares en daños en 2020**. Es hora de adoptar un nuevo enfoque para evitar que el ransomware afecte a su empresa.

**5x** Crecimiento del ransomware entregado a través de SSL en los últimos seis meses<sup>1</sup>



## Descifre, detecte y prevenga amenazas en todo el tráfico SSL

Los adversarios eluden los controles de seguridad heredada ocultándose en la encriptación SSL.

### Diferencia de la arquitectura del proxy:

Descifre y detecte las amenazas en todo el tráfico SSL con escala en la nube y capacidad informática masiva.

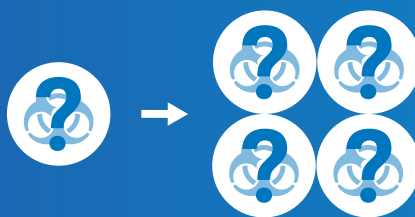
## Ponga en cuarentena los ataques desconocidos y detenga el malware paciente-cero

Los atacantes superan las defensas basadas en la firma, creando cargas útiles para cada objetivo.

### Diferencia de la arquitectura del proxy:

Detenga los ataques de paciente-cero con la cuarentena impulsada por inteligencia artificial que retiene el contenido sospechoso para su análisis, a diferencia de los enfoques de paso heredados basados en cortafuegos.

**4x** Aumento de variantes de ransomware nunca antes vistas en 2020<sup>2</sup>



## Seguridad uniforme para todos los usuarios y todos los lugares

El ransomware no discrimina en base a la ubicación; necesita una seguridad uniforme en toda la empresa.

### Diferencia de la arquitectura del proxy:

Asegúrese de que todos los usuarios tengan la misma gran seguridad todo el tiempo, tanto si están en casa, en la oficina central o de viaje.

**38%** Aumento del tráfico remoto<sup>3</sup>



## Reduzca instantáneamente su superficie de ataque

Los adversarios confían en la capacidad de pivotar y trasladarse lateralmente a través de las redes planas heredadas para tener éxito.

### Diferencia de la arquitectura del proxy:

Empiece desde una posición de cero confianza, donde no se pueda producir movimiento lateral. Las aplicaciones son invisibles a los atacantes y los usuarios autorizados acceden directamente a los recursos necesarios, no a toda la red.

**60%** Eliminarán progresivamente las VPN para el acceso a la red de confianza cero (ZTNA) para 2023<sup>4</sup>



## Evite el ransomware antes de que comience

Dé el paso a un enfoque fundamentalmente diferente para detener el ransomware con **Zero Trust Exchange de Zscaler™**.

[Más información hoy](#)

<sup>1</sup> Zscaler ThreatLabZ Research, septiembre de 2020  
<sup>2</sup> Ibid.  
<sup>3</sup> Statista  
<sup>4</sup> Gartner Market Guide for Zero Trust Network Access