

INFOGRAFÍA

Confianza cero: la defensa definitiva contra el ransomware



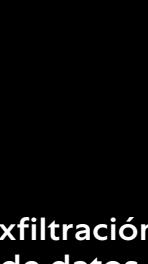
Los cambiantes ataques de ransomware sortean la seguridad tradicional de la red

A medida que los usuarios, las aplicaciones y los datos se han ido liberando del perímetro en los últimos dos años, el alcance y el impacto del ransomware se han acelerado. Los atacantes individuales se han visto sustituidos por grupos que compran y venden entre sí conocimientos y paquetes de herramientas especializados. Los ataques, que antes eran amplios y unidimensionales, ahora utilizan tácticas selectivas y de varios niveles que son casi imposibles de detener con las arquitecturas de seguridad tradicionales de castillo y foso.



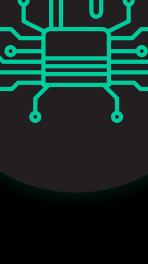
20 000 millones de dólares estadounidenses

daños estimados como consecuencia del ransomware en 2020



Cada 14 segundos

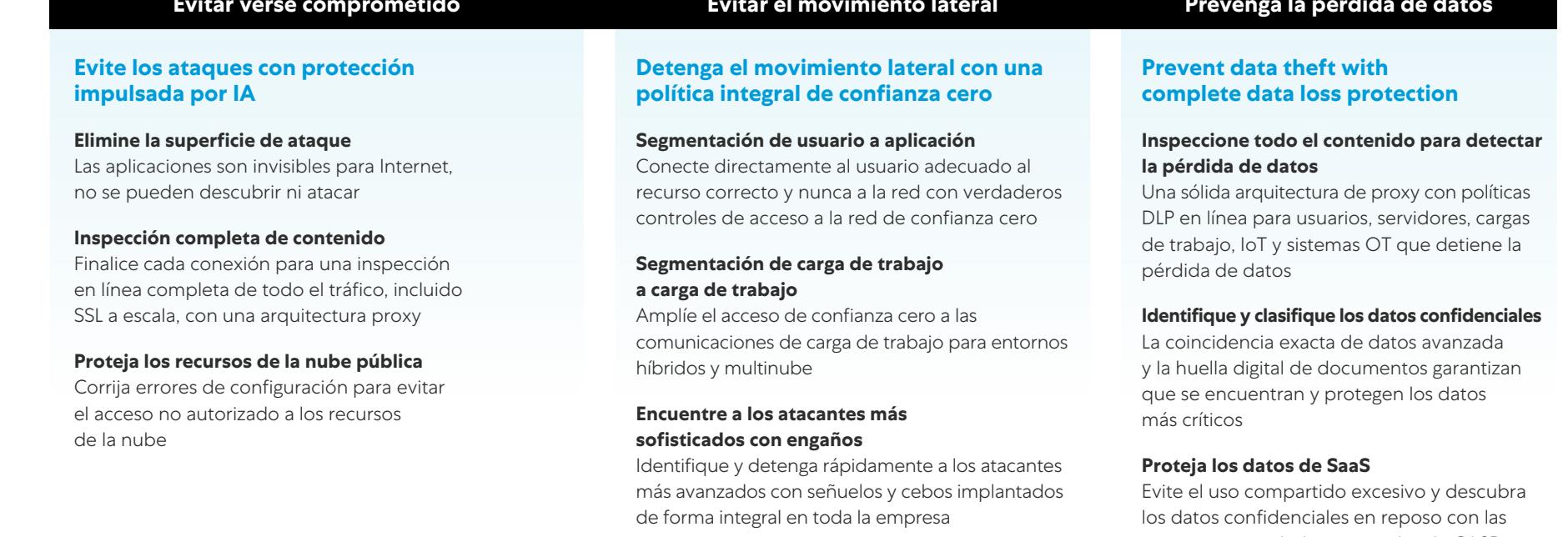
se produce un ataque de ransomware en alguna parte del mundo



500 %

aumento del ransomware oculto en SSL para eludir las defensas tradicionales

El ransomware es el mayor riesgo para las empresas digitales:



80 %

de los ataques comienzan con un correo electrónico de phishing

94 %

de las infecciones tardan menos de 4 horas en propagarse

50 %

de todos los ataques de ransomware son violaciones de datos

200 %

aumento del tiempo de inactividad por culpa del ransomware

234 000 dólares estadounidenses

pago promedio de ransomware

Arquitectura de confianza cero



Confianza cero: la estrategia más eficaz para la protección contra ransomware

Prevención superior frente al ransomware:

La inspección en línea de todo el tráfico para las empresas actuales que dan prioridad al servicio móvil y a la nube minimiza la superficie de ataque y elimina el movimiento lateral.

Deje atrás las soluciones tradicionales:

La confianza cero ofrece un enfoque completamente diferente a las arquitecturas de seguridad de red tradicionales de tipo castillo y foso, ya que conecta directamente a los usuarios con las aplicaciones, nunca con la red.

Seguridad que ayuda a la empresa a funcionar:

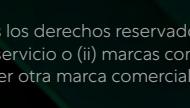
Reduce la complejidad y los costos con un modelo de seguridad totalmente entregado en la nube que elimina la infraestructura tradicional y potencia la agilidad empresarial y la experiencia del usuario.

Resultados empresariales y de seguridad de adoptar la confianza cero

Reducción de riesgos sin igual

Elimina la superficie de ataque y el movimiento lateral con una protección superior de los datos y frente a amenazas ciberneticas

35 x
reducción de máquinas infectadas



Menor tiempo de obtención de valor

Implantado como un auténtico servicio en la nube sin ninguna infraestructura, se puede poner en marcha en menos de 24 horas

Implementado por más de

10 000 usuarios

en menos de 48 horas

NORDSTROM

Mejor valor

Elimina los productos puntuales de seguridad y simplifica las operaciones

70 %
reducción de costes

SIEMENS

Fuente: <https://www.unireads.com/solutions/ransomware-education>

Ler el libro electrónico →

©2021 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y Zero Trust Exchange™ son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca comercial es propiedad de sus respectivos propietarios.