Factores clave por los que implementar Zero Trust

Dado que los ciberataques son cada vez más frecuentes y sofisticados, las organizaciones deben hacer todo lo posible por reforzar sus defensas. Implementar una estrategia Zero Trust es un paso muy importante, pero además las empresas deben gestionar los cambios tecnológicos y las expectativas de los usuarios en ese proceso.

Cada 2 segundos

Aumento de las amenazas

es la frecuencia con la que una empresa, un consumidor o un dispositivo tendrá que enfrentarse a un ataque de ransomware en 2031

Cybersecurity Ventures Ransomware Market Report

31 %

La región EMEA, en el punto de mira

es el porcentaje de víctimas de ransomware de la región EMEA, la segunda con el mayor porcentaje, del 1 de mayo de 2021 al 30 de abril de 2022

Informe de Akamai sobre amenazas de ransomware en la primera mitad de 2022

41 %

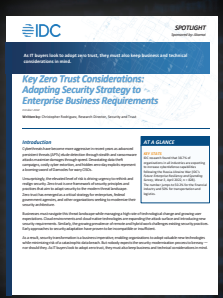
Centrar las defensas

es el porcentaje de participantes en la encuesta de IDC de abril de 2022 que identificaron la seguridad de red como principal foco de atención a medida que aumentaban sus capacidades de ciberdefensa

IDC Spotlight Key Zero Trust Considerations (estudio patrocinado por Akamai): Adapting Security Strategy to Enterprise Business Requirements, doc #US49728722, octubre de 2022

Ventajas para la empresa del modelo Zero Trust

- Combatir el ransomware
- Proteger el entorno de trabajo híbrido
- Satisfacer los estándares de cumplimiento
- Proteger la migración a la nube


IDC

SPOTLIGHT

Key Zero Trust Considerations: Adapting Security Strategy to Enterprise Business Requirements

AT A GLANCE

Introduction

Lea el estudio de IDC Spotlight, patrocinado por Akamai: Key Zero Trust Considerations: Adapting Security Strategy to Enterprise Business Requirements, doc #US49728722, octubre de 2022, para obtener más información.

Disponible solo en inglés

Leer el estudio de IDC Spotlight

 | Asistencia | Publicado en febrero de 2023