

7 Tendencias de Ransomware Que usted necesita conocer

Cada día hay nuevas historias de ataques de ransomware que paralizan las organizaciones y cuestan millones, y a medida que el mundo avanza en trabajar bajo la modalidad a distancia, esta situación parece no tener fin.

Pero, ¿hasta qué punto es grave? Considere:

95% de las organizaciones tienen soluciones de seguridad para prevenir y/o mitigar los ataques de ransomware, pero...

63%

ha sido víctima de un ataque de ransomware en el último año.

&

33%

ha sido víctima en el último mes.

38%

ha perdido alrededor de una semana de productividad desde el descubrimiento hasta la remediación.

&

24%

Perdió más de un mes.

¿Y lo que más asusta?

89%

de los profesionales de TI han notado un aumento de los ataques de ransomware en el último año, siendo los portátiles, desktops y dispositivos móviles los más atacados.



¿Y ahora qué?

Para apoyar a los trabajadores remotos y mitigar la amenaza del ransomware, el **84%** de las de las organizaciones están de acuerdo en que un marco de seguridad Zero Trust es el camino correcto a seguir. Sin embargo, sólo el **43%** tiene un marco de seguridad Zero Trust totalmente implementado.

84%

Mientras esta discrepancia exista, más de la mitad de las organizaciones mundiales seguirán siendo susceptibles de sufrir ataques que pueden paralizar la productividad y costar millones de dólares en daños.

43%

¿Por qué ser uno de ellos?

[Descubra cómo Zero Trust ayuda a defenderse del ransomware](#)