ivanti

7 tendenze del ransomware che devi conoscere

Ogni giorno porta con sé nuove storie di attacchi ransomware che paralizzano le organizzazioni e costano milioni. E ora che il mondo si sposta verso il lavoro a distanza, pare proprio che il fenomeno non accenni ad esaurirsi.

Ma quanto è grave? Vediamo:

Il 95% delle organizzazioni dispone di soluzioni di sicurezza per prevenire e/o mitigare gli attacchi ransomware, ma...

Nell'ultimo anno,
Il 63%
è rimasto vittima di un attacco ransomware.

&

Nell'ultimo mese, ne è rimasto vittima
Il 33%

Il 38%
ha perso circa una settimana di produttività, dalla scoperta alla risoluzione.

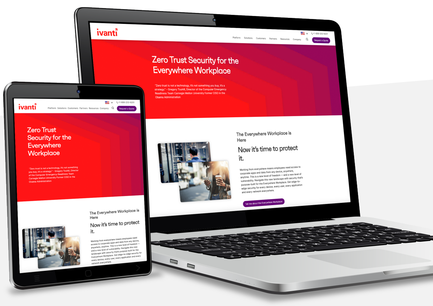
&

Il 24%
ha perso più di un mese.

Non basta ancora?

89%

Nell'ultimo anno, l'**89%** dei professionisti IT ha notato un aumento degli attacchi ransomware, e laptop, desktop e dispositivi mobili si sono rivelati i dispositivi più presi di mira.



E ora?

L'**84%** delle organizzazioni concorda sul fatto che un framework di sicurezza zero trust costituisca la strada giusta per supportare la forza lavoro remota e mitigare la minaccia del ransomware. Tuttavia, solo il **43%** dispone di un framework zero trust completamente implementato.

84%

Fino a quando tale discrepanza non verrà colmata, più della metà delle organizzazioni globali rimarrà vulnerabile a quel genere di violazioni che possono bloccare la produttività e costare milioni di dollari di danni.

43%

Perché essere una di loro?

Scopri come lo zero trust aiuta a difendersi dal ransomware

La ricerca in questa infografica è stata condotta tra il 30 aprile e il 29 maggio 2021 da MSI-ACI tramite un questionario online somministrato a 1.005 professionisti dell'IT negli Stati Uniti, nel Regno Unito, in Francia, Germania, Australia e Giappone.