itnews ASIA

Supported by BeyondTrust

Zero Trust Priorities for APAC Companies

Companies progressing their adoption journey

The term Zero Trust has been used as a buzzword in the IT industry, but it continues to be considerably vague when it comes to adoption strategies.

According to NIST definitions, the main goal of Zero Trust is to "prevent unauthorised access to data and services, coupled with making the access control as granular as possible", and this is very important for the modern workplace.

With the change in the traditional workplace, where the industry witnessed an explosion of remote staff and essential third-party remote connections (e.g. supply chain, IT support), deploying the Zero Trust fundamentals by limiting privileges has become more critical than ever.

To find out the state of Zero Trust in a perimeter-less digital world, BeyondTrust partnered with iTNews Asia to survey 102 IT and business leaders across Asia on their experiences with cyber security and their preparedness to mitigate the challenges.

The research found business and IT leaders are aware of Zero Trust, and increasing the implementation of Zero Trust is a top cybersecurity priority for the next 12 to 18 months.

However, while a third of respondents said reducing endpoint security threats is a priority, Windows endpoints still lag behind Mac endpoints and Linux servers when it comes to removal (or planned removal) of local admin rights from users. This leaves organisations vulnerable to threats that leverage these very privileges.

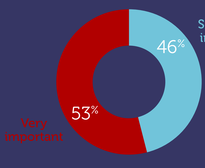
Here's what else we learnt...

#1 *Increasing the adoption of Zero Trust is rated as the top cybersecurity challenge over the next 12 to 18 months.*

The scale of cybersecurity challenges faced over the next 12-18 months

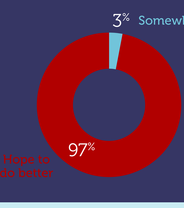
100% *of IT leaders say Zero Trust access is important to their organisation's cybersecurity strategy.*

How important is Zero Trust access to your organisation cybersecurity strategy?



However, ***more than 95%*** *of respondents recognise that they are on a journey and still have a way to go on fundamentals such as least privilege*

Have you catered to the fundamental requirements of Zero Trust such as authentication, compliance and least privilege in your budgetary and procurement plans?



1 in 2 *say cyber protection is the key driver to initiate or augment Zero Trust identity management*

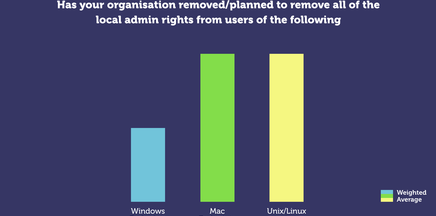
1 in 3 *see reducing endpoint security threats as a key driver to initiate or augment identity and access management within a Zero Trust framework.*

What are the key drivers for your organisation to initiate or augment Zero Trust identity management

REMOTE IS HERE TO STAY:

67% *of respondents see securing 3rd party remote access as a key challenge, while* ***half*** *say that securing remote workers will continue to be a challenge*

Has your organisation removed/planned to remove all of the local admin rights from users of the following



About the survey

This survey was conducted in September and October 2022 by iTNews Asia of 102 IT and business leaders across Asia from 14 different industry sectors from organisations with more than 100 staff.