Going Fearless with Zero Trust

Jul 8, 2022

Authored by Tushar Haralkar, Security Software Technical Sales Leader, IBM Technology Sales, India/South Asia

Businesses today are under a tremendous pressure to keep customers happy. To do so, they are having to make services accessible whenever and wherever customers choose to access them. This is especially relevant today, as there has been a considerable rise in digital interactions, driven by remote working, during the pandemic.

The result?

Your data, applications, and users are everywhere, and there are exponentially more endpoints for IT teams to support - but with reduced visibility. Moreover, devices, users, and data are inter-linked like never before, increasing the risks.

It thus becomes important to create a stronger security posture that limits potential risk. And, to protect what has become a scattered ecosystem, enterprises require correlation of real-time security context across all security domains.

Now, here comes the twist.

Security traditionally relied on the perimeter. But remote work and the rise of multi-cloud have led to the traditional boundary being evaporated. In fact, according to the 2022 IBM Security X-Force Threat Intelligence Index, Asia was the most targeted region for cyberattacks in 2021 and India was among the top three most attacked countries in the region. Cybersecurity is now a perimeter-less world where users are accessing data from anywhere, any place, and any device.

And that is where zero trust approach to security comes in.

It assumes that every entity, connection, or endpoint is a threat. It can help organizations modernize operations and allow security to become a business enabler by dynamically adapting to users, datasets, and workloads throughout the business – no matter where they are.

Not surprising then that zero-trust security has emerged as the new normal of cybersecurity. To dive on this deeper, we recently collaborated with the Times of India for a Times Techies webinar, where I was joined by leading industry experts **Mayank Vaish, Vice President, Identity and Access Management, Aujas** and **Nilesh Shirke, Associate Partner, EY**.

Offering additional insights on zero trust and IBM’s role in helping customers undergo their zero trust journey, **Aujas’ Mayank Vaish** says, “The core of zero trust architecture is based on a robust identity layer and strong access control policy engine. With a wide range of open standards for identity authentication and authorization, and a very flexible Identity and Access Management (IAM) policy engine, IBM's IAM solutions fit very well in the zero trust architecture of organizations. In fact, IBM has been offering these core zero trust elements in its Security portfolio much before the name 'Zero Trust' started trending.”

EY’s Nilesh Shirke adds, “Organizations’ resources are scattered in the hybrid cloud infrastructure with different levels of visibility and control. The IBM zero trust security strategy can help organizations to manage the risks of disconnected environments, while allowing valid users access to the right resources. IBM’s zero trust model enforces contextualization required to securely connect the legitimate users to the right data at the right level of accesses so that organizations are protected from cyber threats.”

To know more on the highlights of our discussion, please read the Times of India article here.

Blog Categories

Secure