Got something to say?
If you have any comments to make on this issue, please e-mail: david.ndichu@itp.com

Vijay Saradhi

Containerisation: model for BYOD

"Containerisation, in simple words, is like putting a brick wall between corporate data or apps, and personal data or apps used by the employees."

Vijay Saradhi, evangelist, ManageEngine

Bring Your Own Device (BYOD) approach helps organisations not only save time and overhead costs on managing company-owned devices, but also boosts employee morale as they can work from anywhere thereby increasing their productivity and response times.

A few years ago, companies provided employees with mobile devices for official use so that they could monitor and control any sensitive company information ordata that might have been stored on these devices. The company managed every aspect of the mobile device and the information stored on it. Times have changed. Not only have employees moved towards an all-purpose device approach, but even IT departments have recognised the need for managing strategic currency (data) over strategic resources (mobile phones).

Today's business advantage lies in leveraging mobility as a competitive advantage. Even if companies don't adopt mobility practices, employees still tend to use their devices on company premises and this creates a security risk that might hamper business data.

We would certainly recommend the BYOD approach as it helps organisations not only save time and overhead costs on managing company-owned devices but also boosts employee morale as they can work from anywhere thereby increasing their productivity and response times.

However, along with these benefits comes organisational challenges and threats such as loss of devices, scalability and security vulnerabilities. To secure corporate data on employee devices, organisations need to provide an abstraction layer over the raw data, which also enables resources such as documents and applications to access the data easily.

With BYOD, the lines are blurred between professional and personal, where employees are concerned about their privacy and personal data. In this scenario, containerisation is the only way forward.

Containerisation, in simple words, is like putting a brick wall between corporate data or apps and personal data or apps used by the employees. It is simply installing apps to create isolated compartments or containers on employees' personal devices, where the organisation can provide a secure environment, which can be controlled by them. As a risk mitigation strategy, organisations need to partition the personal and corporate data on the employee device into containers, where the flow of information between each container is restricted.

Containerisation gives IT admins the tools needed to establish separate, encrypted, policy-enforced containers within personal devices, and to deliver email, browser apps, and data specifically to those containers. IT policy and management extend only to the container's contents, which reside in complete isolation from the rest of the device. If a device is lost or stolen, IT can wipe the containers without disturbing personal assets. This provides robust information integrity, while preventing data leakage.