5 Enterprise Security Tips for a Hybrid IT World
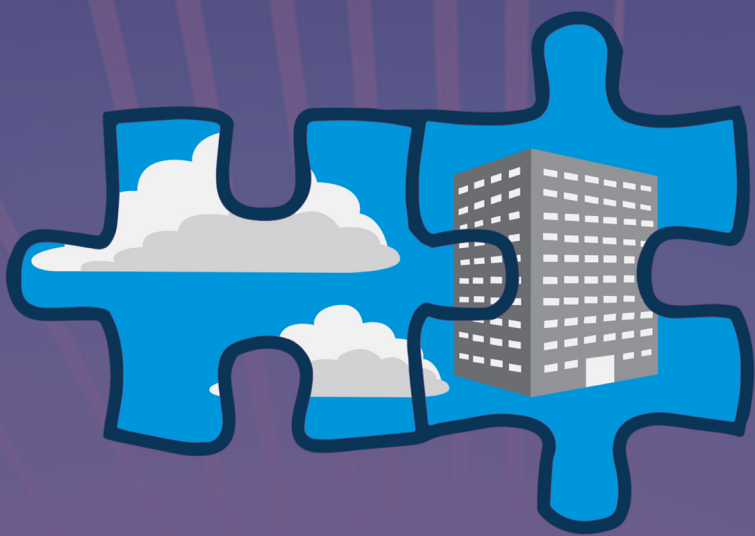
1. Demand transparency from your CSP

Cloud service providers (CSPs) should have clear documentation concerning policies for the accessing, modification, replication and deletion of data.

67% of IT Decision Makers have security concerns about their cloud provider.[1]

2. Implement Multifactor Authentication

Hackers and unauthorized users can attempt to infiltrate cloud services from anywhere, opening up your enterprise to credential stuffing attacks.

38% of hackers considered MFA the toughest security system to beat.[2]

3. Encrypt important data in the cloud
(Data in transport and at rest)

Users should always connect to cloud resources through a secure connection that is encrypted by a certificate assigned by a trusted certificate authority in order to prevent session hijacking and man-in-the-middle attacks.

50% of companies are concerned with their enterprise mobility security strategy.[2]

4. Manage hybrid IT security through a single security management console

The solution should be able to capture data from both cloud and on-premises systems to help quickly identify, contain and mitigate threats. Cloud admins should be able to roll out security policies as quickly as they can spin up additional servers and resources.

Hybrid IT
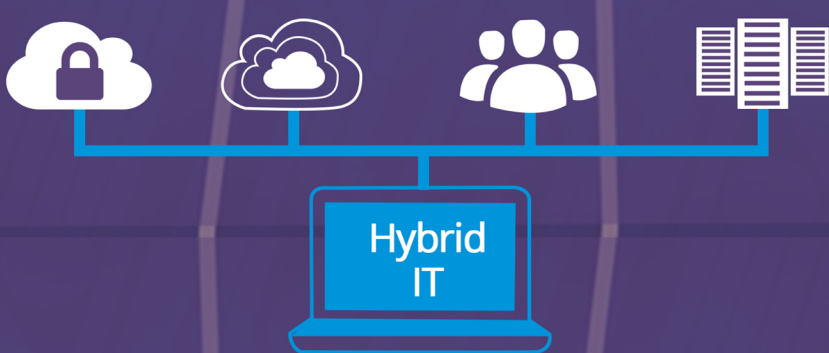
40% The percentage of apps and platforms residing in on premises systems in a typical IT department.[3]

5. User carelessness can compromise data

Selecting a cloud provider with integrated information protection or a rights management system will help prevent user oversights. These types of systems classify your stored data and then implement policies that pertain to the assigned classification.

61% Are concerned with how employee mobility affects enterprise security at their organization.[2]

WEI Dedication meets innovation.

Ask WEI to review your Hybrid IT strategy and your cloud security strategy to help identify possible vulnerabilities.

www.WEI.com   (800) 296-7837

Talk to WEI Today!