7 Reasons to keep applications & data on-premise

Chris Tucker, VP Customer Engagement at MBX Systems

The question of whether enterprise applications and data should be deployed behind the corporate firewall, in a public cloud, or in a hybrid environment is a source of ongoing debate. There is no one-size-fits-all answer for every application or every company. These decisions must be made on a case-by-case basis as each organisation formulates its cloud strategy.

Indeed, even with the stampede to the cloud, the on-premise model remains not only a viable alternative but in some cases a preferable one. That's why Oracle's Larry Ellison recently told investors that on-premise and cloud data centres will co-exist for decades, "if not forever". It's also why many developers who utilise a Software-as-a-Service (SaaS) delivery model also offer an on-premises option – frequently pre-loading their software on purpose-built server appliances that preserve key SaaS benefits by eliminating software installation and configuration.

A variety of factors can tip the scales away from a cloud deployment and toward an on-premise implementation, whether on a traditional network or as part of a private or hybrid cloud. They include:

1. Need for continuous end-user access

Applications or data running or stored in a public cloud cannot be accessed if the office Internet connection goes down. If continuous 24/7 access is critical, in-house deployment may be a safer way to go.

2. Regulatory compliance issues

If you're in an industry sector like healthcare and financial services that must adhere to government-imposed data security regulations, it is frequently easier to prove that sensitive data is secure if it is kept behind the firewall.

3. Data traceability

The precise location and file movement of data stored in a public cloud can be tough to pinpoint. In one recent survey, 53% of respondents reported difficulty accessing log files and other forensic artifacts for information handled by cloud service providers. On-premise deployments typically enable better traceability.

4. Global access limitations

A global organisation may have to grapple with bandwidth constraints and restricted Internet access in some countries where it operates. In these cases, private WAN connections to in-house data centres can be more reliable than public cloud offerings and dependence on Internet access.

5. Cloud latency

Organisations and end users frequently cannot tolerate performance delays caused by the unpredictable nature of the various network connections that sit between on-premise and cloud applications. In cases where these delays are unacceptable, the on-premise option wins.

6. Cross-border complications

Germany's data protection law already prevents data storage outside of the country, and some observers have speculated that the new EU Data Protection Regulation may lead to similar mandates by each country in the EU. That could drive more application and data storage deployments in-house, particularly for companies that operate globally.

7. Distrust of cloud providers

Despite advances in cloud security, some IT teams believe they are better equipped than cloud providers to prevent security breaches by managing applications and data in-house.

At the end of the day, the on-premise versus cloud decision boils down to control. But, at least over the short term, there are compelling reasons to choose the on-premise route in certain scenarios. The cloud has its place, but not all roads lead there. ■

Related video:

MBX Systems at IP EXPO Europe

Enterprise Management 360°

Watch video ▸

▲ BACK TO TOP