Application Hosting by Application Developers

In today's economic environment, customers are looking to reduce expenditure. Having an application provider host their application seems an excellent way to reduce costs, as it is often cheaper than having a service provider like Logical host 3rd party applications.

How do we identify proper cloud applications?

This is a commonplace of confusion. Cloud-based applications are built from the ground up to be used across the internet and won't use a terminal server. If most cases, it will be Web-based. An excellent example of a properly built cloud application is the Zero accounting system. Adopting a non-cloud-based application to a proper cloud application is a TOTAL re-wite and involves a significant effort on behalf of the application provider.

Many application providers use a quick and dirty solution by providing a terminal server-based application and calling it a cloud application. A Terminal server is the same as running the application on your own server, but the server is based on your application providers hosting services. By the very nature of the way this works, this is NOT a proper cloud-based solution and brings other issues, as discussed in this document.

The first issue is security.

In most situations, the application providers use direct RDP access across the Internet to access the environment, only being secured via the source IP address.

What this means is that the connection to the service is secured by the computer network address you are coming from. These are easily falsified and NOT considered secure,

All applications accessed across the Internet require some tunnel encryption before user authentication is requested.

The NZ government outlines security standards for these type of connections and are very clear that direct connections to a terminal server are not acceptable: https://www.cert.govt.nz/business/guides/securing-your-internet-exposed-rdp-server/

Printing is often sent directly via redirected ports from a customer's router, another significant security shortcoming. As you can imagine, the information being printed is often of a sensitive nature and using this method is exposing that information to the world.

On many modern computer networks, the network services and devices are secured via a central user directory service. This works well when you have a cohesive, well-designed environment. If you add a remote, isolated terminal server in the mix, this, in most cases, is simply not possible.

The Second issue is functionality.

Most businesses likely require more than a single application to carry out the full functions of the company. Other applications like Word, Excel and Outlook are required for the company to function fully. Because the applications are being hosted off-site, in isolation, getting data to and from other applications is difficult and near impossible. This usually means the customer has data all over the place with no central point of management or backup.

Customers get themselves into these situations through a lack of "big picture" understanding and believing salespeople who, in many cases, are only interested in achieving sales.

What is the difference with the Logical Solutions Terminal server Approach?

When Logical Solutions provides a "Terminal Server" solution for its customers, we look at the customer's whole computing environment rather than single applications in isolation.

Our responsibility is to the customer's total environment, rather than a single application in isolation. Many application providers want you to think "all you need is their application", but, for most businesses, there are services required from multiple vendors needed, and they all need to be able to work together.

If you have an application being hosted on an isolated server remotely, achieving the "whole of business" approach becomes very difficult, if not impossible.

Bringing these details to a customer, we are often seen as being obstructive to the customer saving money, and they don't want to know, but we have seen many customers fall into this trap, and the result is the customer is left in a situation where systems don't work as expected.

In these situations, often the customer ends up with a compromised solution and in many cases, has to spend money upgrading hardware because of these decisions. In some situations, the customers have been left with an insecure solution, which is a concern.