appia the cloud at work®

VPNs vs. Cloud Desktops

Many companies and organizations have implemented VPNs for users who need secure remote access to applications and data. This is particularly true when users need remote access to legacy client/service applications, where a typical implementation involves running "thick" client software end-user devices connected through the VPN to a database server.

Why have VPNs been so widely adopted?

They are easy to set up. Most of the time, getting a VPN running is as simple as checking a box on a router or installing an appliance and punching some holes in a firewall.

If VPNs are inexpensive to set up, why should an organization consider replacing them?

They are not easy to manage. VPNs need maintenance, especially for security.

- VPNs do not always use strong authentication or encryption methods.
- If a user has access to the VPN, they can move sensitive data to personal machines, which could already have been be hacked.
- VPN users do not always have strong virus, malware, etc., protection.
- VPN users can access other CPNs or using remote control software when on the VPN.
- Remote user wireless networks are not always secure.
- VPNs do not minimize the bandwidth necessary for optimal performance on slow connections.
- VPNs usually do not create a consistent look and feel across devices.

When you allow VPN access, you really are acknowledging that the least security-minded person in your company now can control your data security. Think about that for a minute. How many links have all your users clicked lately? Were they all secure?

When you look at it, you will see that VPN is not worth the risk.

What are some of the major trends in the industry that are driving companies and organizations to consider replacing VPNs?

In addition to the poor user experience, difficult management, and security, people expect a seamless experience these days, regardless of which device they happen to be using. They do not want to deal with fiddly or unreliable client applications. These trends create huge security, supportability, and user acceptance headaches if a VPN is part of the infrastructure.

VPNs do not address mobility very efficiently. Have you tried connecting to a VPN on your tablet or phone? It works, but it is not pretty.

What options available to replace VPNs?

The cloud desktop is the best option. Cloud desktops give end-users the seamless experience they are looking for; support much better security for the organization, and provide a simple implementation process that just works. It is no surprise to see the rapid rise

in adoption of this technology over the past 18 months. There is every reason to expect it to continue to grow as time goes on.

Other than VPNs, what else can cloud desktops replace?

The great thing about cloud desktops is that many offerings come with technology that will replace distributed encryption software; bring in BYOD and mobility support, and introduce thin devices as an option. All of these save money. Moreover, cloud desktops are much easier to support than distributed machines.

What kind of cost savings can customers and MSPs expect to see?

Typically, the "hard" cost savings are at least 10 to 15 percent per month, and that is before considering the cost of lost or stolen data, the benefits of user mobility, and the protection of data when users. For many employers, these "soft" benefits far outweigh the cost savings.