DIGITAL BOARDROOM IN 5

CIO WaterCooler

How can you secure remote connectivity in a hybrid and multi-cloud world?

Hybrid and multi-cloud offer an excellent way to leverage the best of breed features from all of the different providers. However, this does bring added complexity in terms of security. Neil Briscoe, co-founder and CTO, led this in-depth session on the approaches available to businesses to ensure their hybrid cloud and multi-cloud environments are fully secure.

1

Uptake of remote working technologies (old & new) will increase in a post-COVID19 world; multi-cloud and hybrid-cloud is gaining momentum in parallel – both will have to integrate.

2

Client RAS/VPN, VDI and WAF/ZTNA built in cloud allow for BCaaS and augmentation to existing enterprise estates; with additional benefit of scale-on-demand, pay-as-you-need commercial mechanisms, and integration to LDAP/Active Directory etc.

3

In a multi-cloud/hybrid-cloud world there are 2 common security boundary architectures – central & distributed – both have pros/cons from a cost, political, resource, compliance perspective.

4

Integration of remote working and network security is available – firewalling at network layer based on Active Directory Group etc – works with RAS/VDI/ZTNA; this create granular access to remote users as much as when on-net.

5

VDI is increasing rapidly; reasons – zero-trust, can be truly BYOD, any device type, "golden image" creation, Windows Virtual Desktop with Multi-session licensing now available.

"Is the cloud more secure as your own data centre – No. But can it be. Absolutely yes! With the right tools."

Neil Briscoe, co-founder and CTO, Cloud Gateway