BLUE SKY THINKING

How Private Cloud Can Solve
Your Security Problems

The International Data Corporation (IDC) has said that it expects this year to be the "year of multi-cloud" as the pandemic reaffirms the critical need for business agility. By the end of 2022, the organisation predicts that enterprises around the world will be relying on a delicate mix of public cloud, on-premise servers, private cloud and legacy solutions as they begin to migrate to a more agile infrastructure that paves the way to hybrid working. According to Gartner, there was a global surge in cloud adoption across a diverse range of industries in 2020, but one thing holding businesses back - particularly those in highly sensitive industries like finance - is concern around data security. There's an erroneous school of thought out there that an on-premise solution is better for businesses that are concerned with security. When compared to a public cloud solution, such as those offered by Amazon, Google and IBM, that may well be the case. But as the sophistication of private cloud servers continues to evolve, it's become the preferred solution for storing data in a way that's safe, secure and compatible with hybrid working.

THE PROBLEM WITH LEGACY SOLUTIONS

Traditionally, businesses use on-premise equipment such as HDDs or disk-based storage, or even an on-premise server to channel data and services to those that needed to access it in the office. However, now that we're gearing up for a post-pandemic landscape that will prioritise remote or hybrid working, deploying on-premise solutions feels like a retroactive step. Not to mention the inherent security and backup risks of storing data in-house. Data that's stored on-premise might feel more secure, but what happens when there's a fire, a burglary, a power outage or a critical server failure? That data is lost, with very limited backup or recovery options in place to get business back on track. This is where private cloud enters the picture as the de facto solution of choice for businesses that work with important customer data and other sensitive information.

PUTTING SECURITY FIRST WITH CLOUD TRANSFORMATION

Any business could be forgiven for being overwhelmed when it comes to cloud transformation. With so many options spanning public and private cloud, and so many rules and regulations regarding data privacy and protection, it can be difficult to know where to invest long term. The sheer volume of services out there also makes security an inherent challenge, particularly with so many businesses now having to cater for the hybrid working approach. When it comes to devising a data management strategy, the trade-off between accessibility, agility and security is absolutely critical, and is something that will undoubtedly weigh heavily on the shoulders of even the most pragmatic CTOs.

LEAVING ON-PREMISE BEHIND

Once a business has determined that it needs to migrate to the cloud, either because its data backup and recovery strategies can no longer mitigate the risk associated with on-premise solutions, or they're moving toward a more hybrid working environment that demands speed, accessibility and agility, they must decide which path to the cloud to take. Public cloud solutions may have boomed in popularity in recent years for their affordability and accessibility, allowing businesses to effectively 'rent' data service infrastructure for their own storage and computing needs, but they're not ideal for businesses that hold sensitive data like those in the financial sector.

For all the advantages of public cloud solutions, security appears to be the price paid. This can quickly turn into an expensive problem for businesses, particularly as many public cloud providers prefer to share the regulatory burdens that come with data ownership, such as GDPR or PCI DSS. Not only do businesses relinquish an element of control over their data, but they're also still responsible for the manner in which it is stored and can be held accountable when it comes to issues around compliance.

Your **Cloud** Experts

Private cloud is different in that a business has exclusive access to its own cloud infrastructure, usually hosted off-premise by a third-party provider. This allows a business to retain full ownership and control over its data, as well as control over how that data is stored. Because no other client businesses need to be considered, a private cloud's servers can be tailored specifically for a company's individual needs, including all of its required firewalls and policy controls.

By leaving on-premise infrastructure behind and instead opting for a private cloud solution that can be tailored to their own working practices and security policies, companies can blend performance, cost and accessibility without compromising on security.

Find out more at **hyve.com**