

# Azure Virtual Desktop Protection – One page customer deck

AVD Protection – Plan and Implement – 2 weeks

COVID 19 衝擊了全世界，疫情時代人與人之間避免接觸，因此 Work From Home 居家上班取代群聚的辦公室，微軟推出的 Azure Virtual Desktop + M365 協同合作紛或企業採用。然而，佈署完 Azure Virtual Desktop 之後該進行怎樣的安全性配置，才能讓企業使用 Azure Virtual Desktop 辦公之際，可以確保網路與資源的安全性，是一個需要嚴謹看待的課題。

## 【Azure Virtual Desktop Protection 服務的優勢】

透過 MFA、條件式存取進行身分識別

透過 Microsoft Defender for Endpoint、群組原則進行作業系統保護

透過 應用程式控制與 AppLocker 來規範應用程式的使用

透過 Azure Security Center 與安全分數來監測架構安全並修正

透過 反向連線、服務標籤與 Azure Firewall 來規範網路 inbound、outbound 存取

透過 Azure Information Protection 與 Azure Disk Encryption 來保護資料

唯有層層嚴格的把關，Azure Virtual Desktop 才是既便利又安全的 WFH 的行動居家辦公室。

## 【建置流程與項目】

本解決方案進行流程如下：

- 1.解決方案說明與客戶需求討論 (2 工作天)
- 2.授權說明與採購
- 3.解決方案建置 (7 工作天)
- 4.相關設定教學與管理訓練課程 (3 工作天)

解決方案完成時間約 14 個工作天

This solution is only available in Chinese.