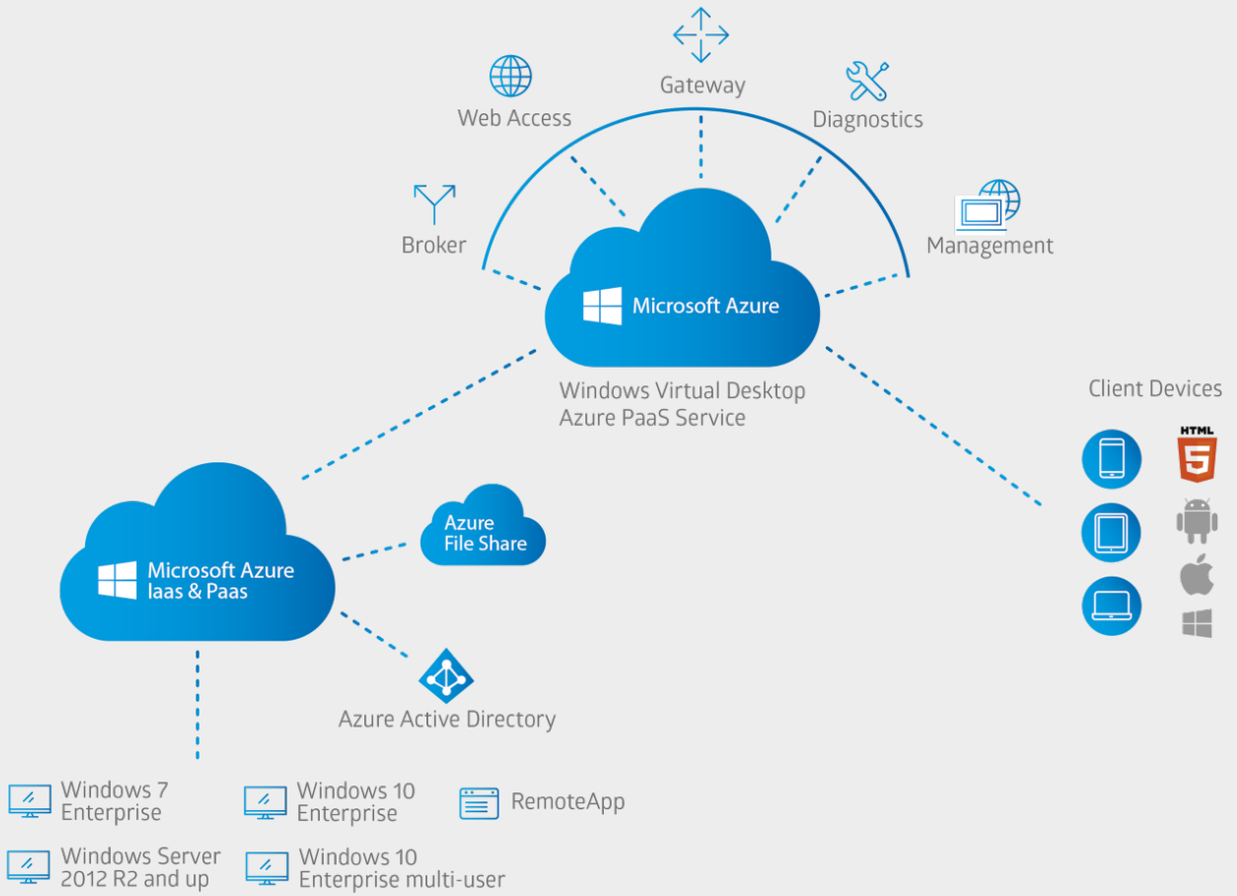
Azure 虛擬桌面



任何終端設備就能隨處存取虛擬桌面

簡化作業、數分鐘完成 AVD 環境佈署

集中管理、彈性擴展、IT 學習成本低

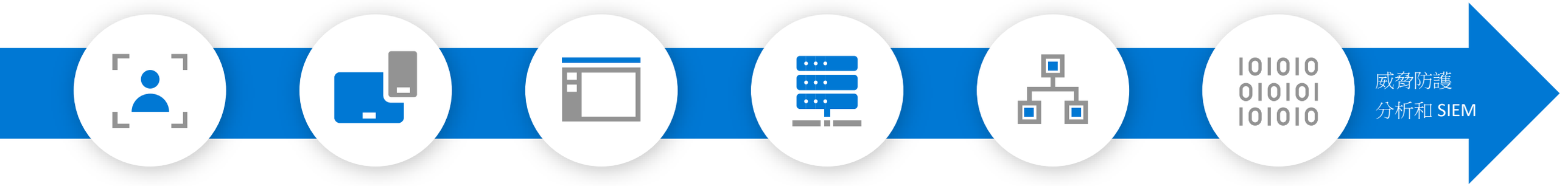
單一平台同時滿足 RDS/VDI 應用情境

Azure AD 安全服務、減少攻擊事件

使用者設定檔容器化、原生 M365 App

Microsoft Azure

Azure 虛擬桌面的安全保護



身分識別

MFA

條件式存取

作業系統

適用於端點的 Microsoft Defender*

原則

應用程式

應用程式控制

AppLocker

基礎設施

Azure 資訊安全中心*

安全分數

Best Practices

網路

反向連線

服務標籤

Azure 防火牆

資料

資訊保護

Azure 磁碟加密

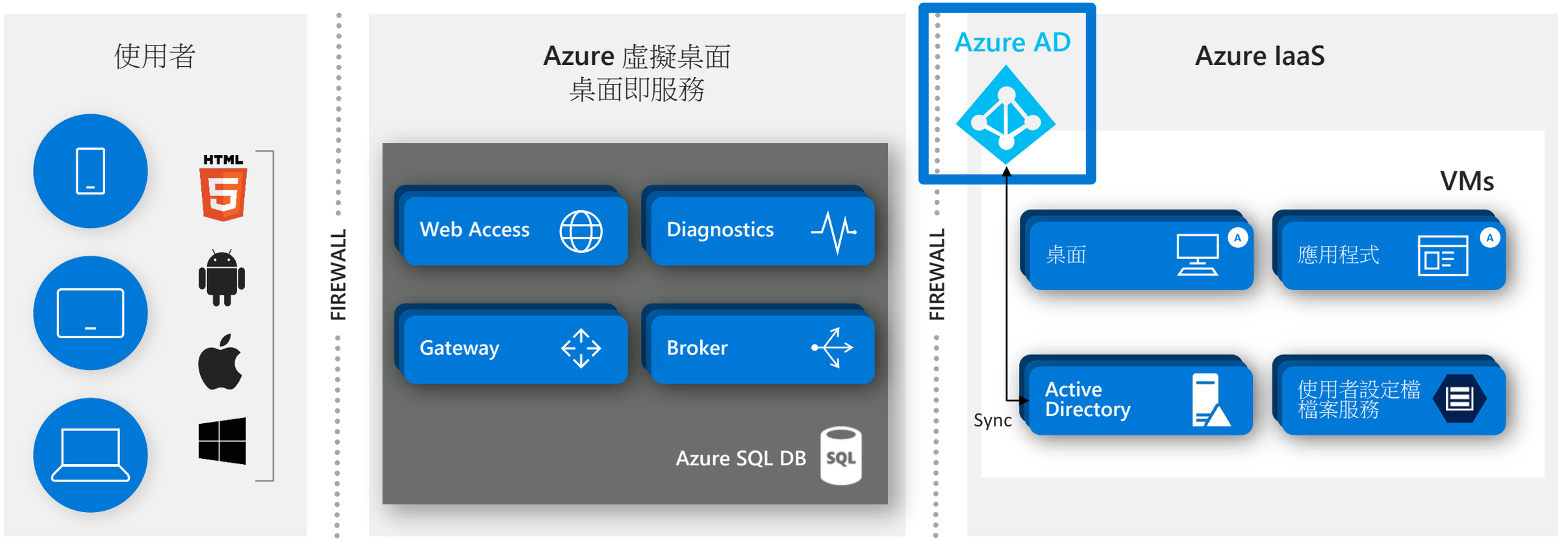
身分識別

身份的安全考慮

Azure AD 用於使用者的身份和存取管理服務

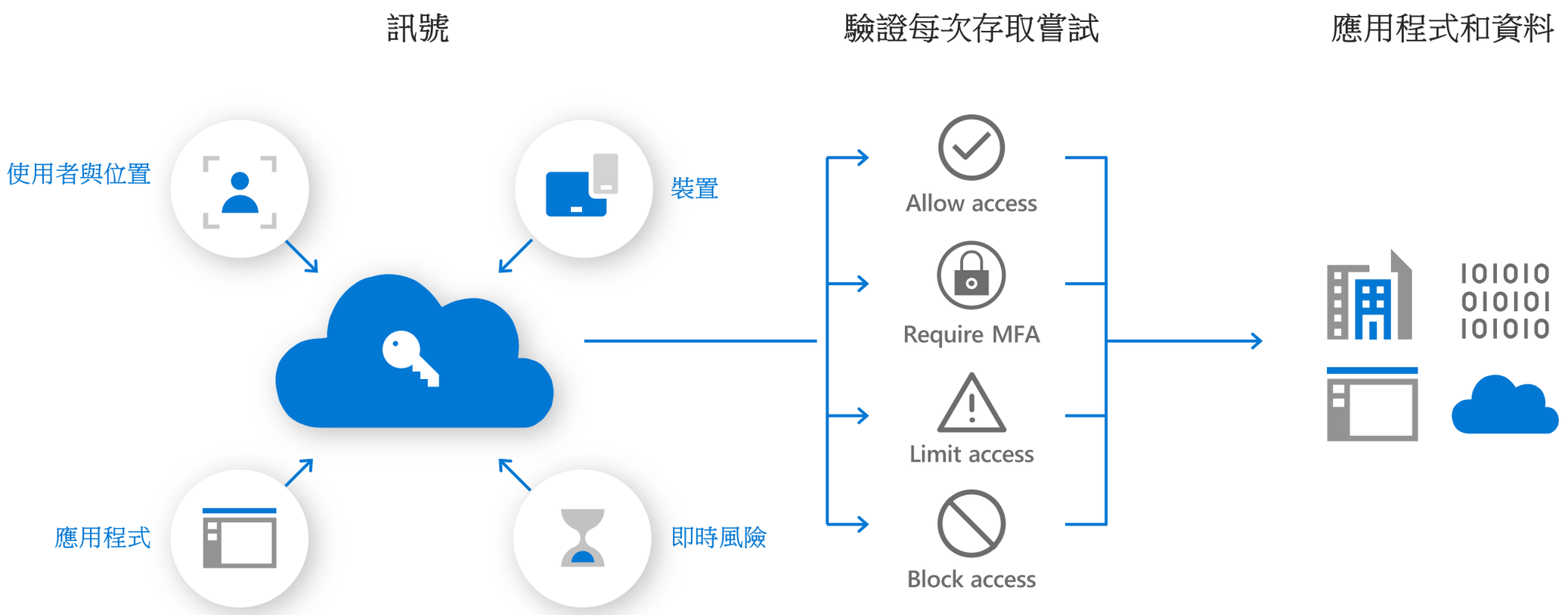
MFA 對於防禦攻擊者存取非常重要

Azure AD 身份保護提供有風險的登入和使用者報告，可與條件式存取一起使用



身分識別 – 條件式存取

實施強有力的保護原則和風險評估



作業系統

Microsoft Defender for EndPoint

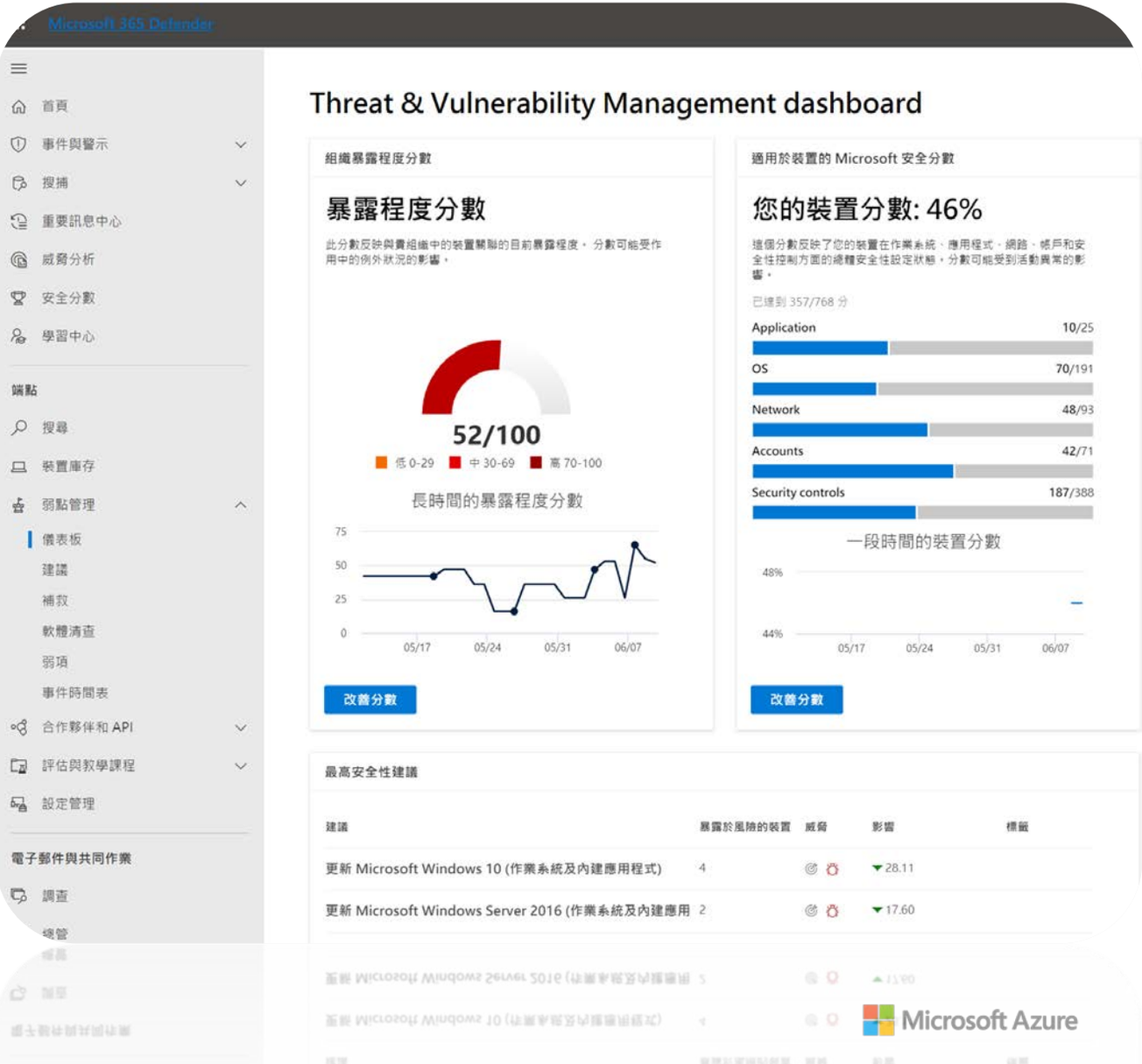
適用於端點的 Microsoft Defender

以風險為基礎的弱點管理和評量

受攻擊面縮小

端點偵測和回應 (EDR)

自動調查和補救



網路 – Azure 防火牆 (標準)

具狀態防火牆即服務

所有流量集中管理

內建高可用性

網路和應用程式流量篩選

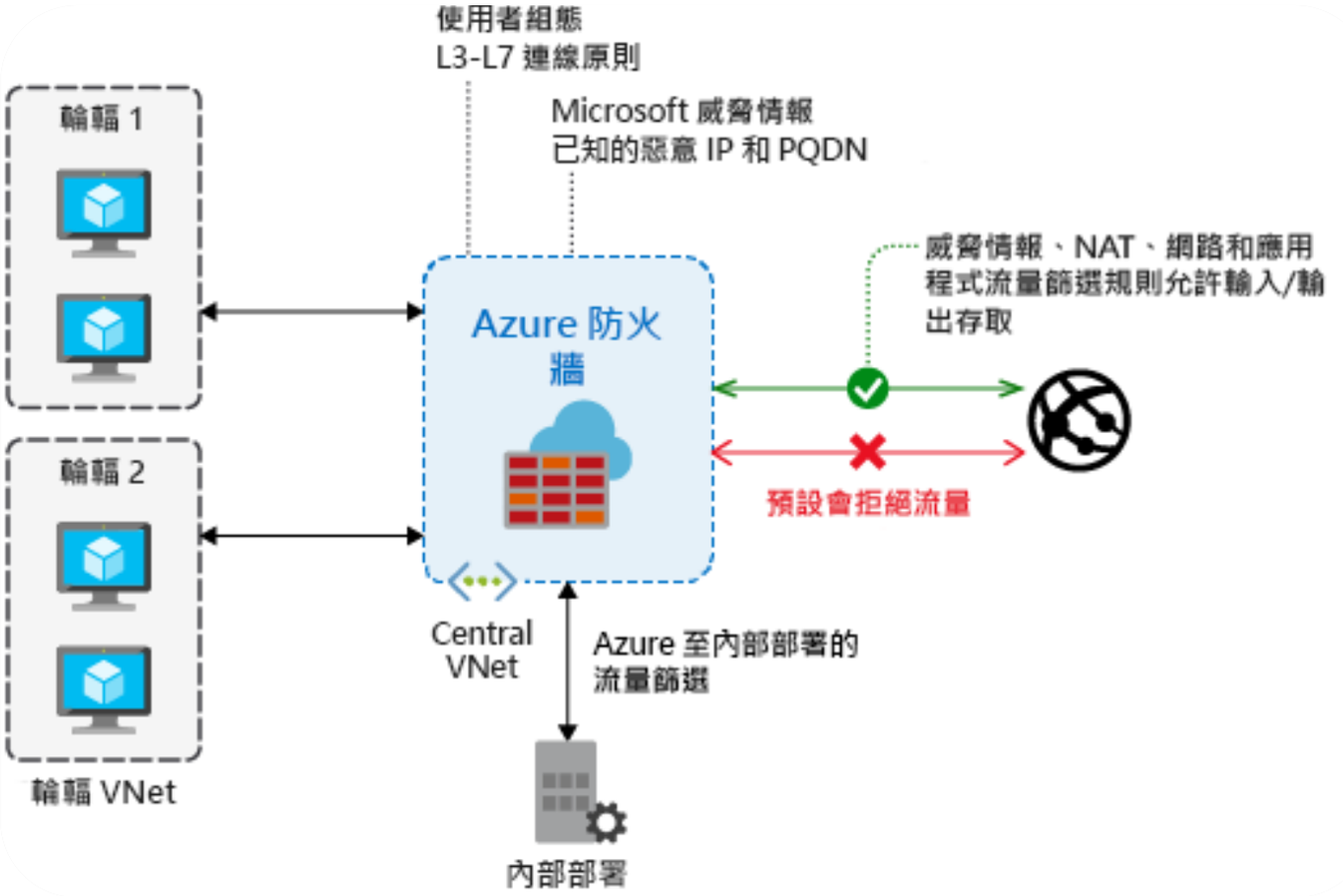
跨 VNet 和訂閱的集中原則

完整的 VNET 保護

篩選 Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)

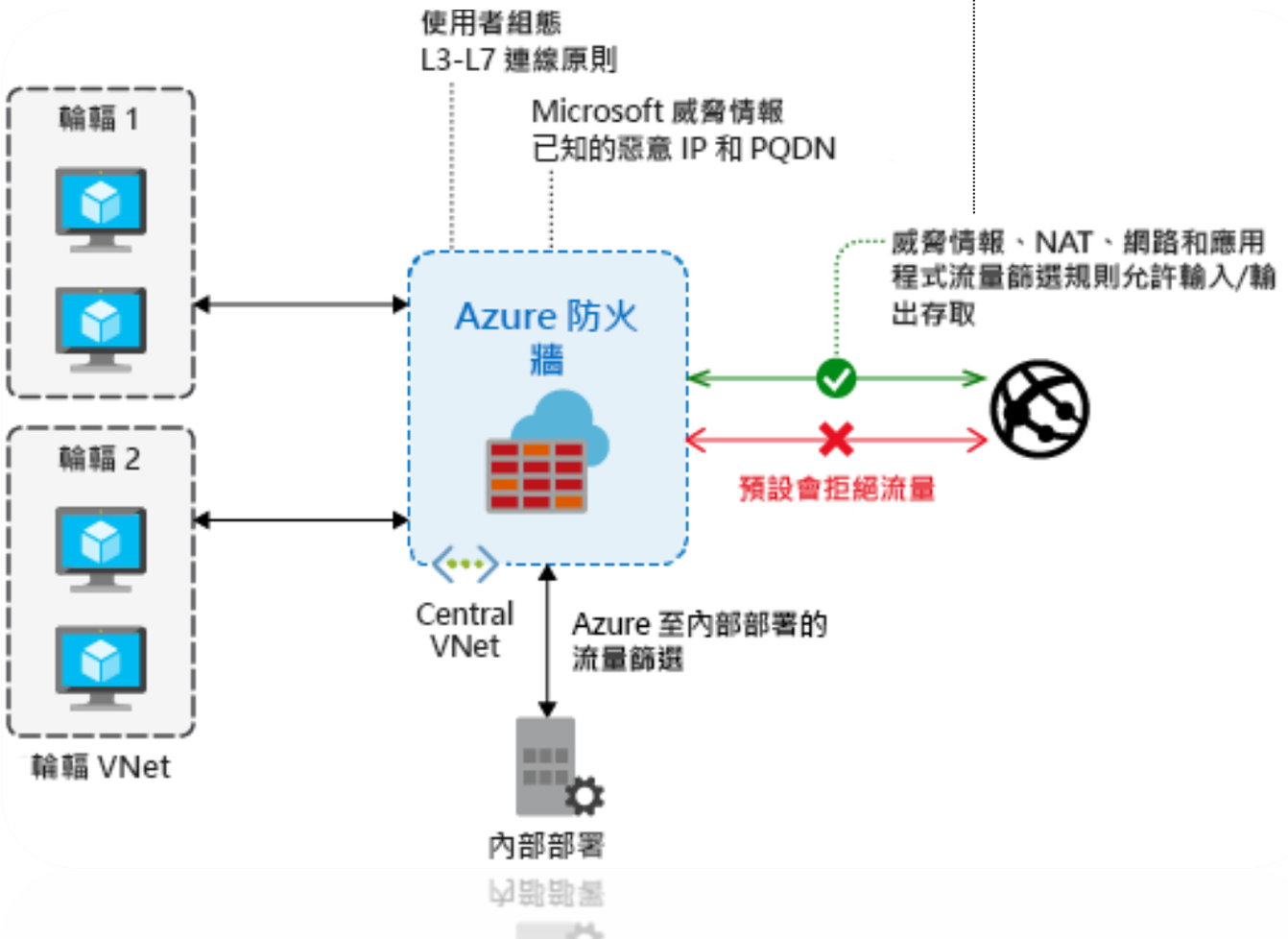
集中式記錄

將紀錄存檔到儲存體帳戶，將事件串流傳輸到事件中心，或將其傳送到您選擇的紀錄分析或安全整合和事件管理 (SIEM) 系統



網路 – Azure 防火牆 (標準)

具狀態防火牆即服務



三個篩選規則

威脅情報

- 提醒並拒絕流入/流出已知的惡意 IP 位址和網域位址的流量。

網路規則

-配置包含來源位址、協定、目的地埠和目的地位址的規則。

應用程式規則

-配置完整網域名稱的功能變數名稱（FQDN），可從子網路存取。

網路 – Azure 防火牆進階 (公開預覽)

雲端原生次世代防火牆即服務

輸出 TLS 檢查

內建對外輸出的 TLS 檢查

客戶通過 Azure Key Vault 整合提供的 Key pair

網路入侵偵測和防護系統 (IDPS)

檢測發出警報並阻止流進/流出惡意流量

支援加密和純文字協定

持續更新的基於簽名的檢測

URL **篩選**

限制使用者存取 HTTP/HTTPS Web 內容

支持 URL 萬用字元

Web **類別**

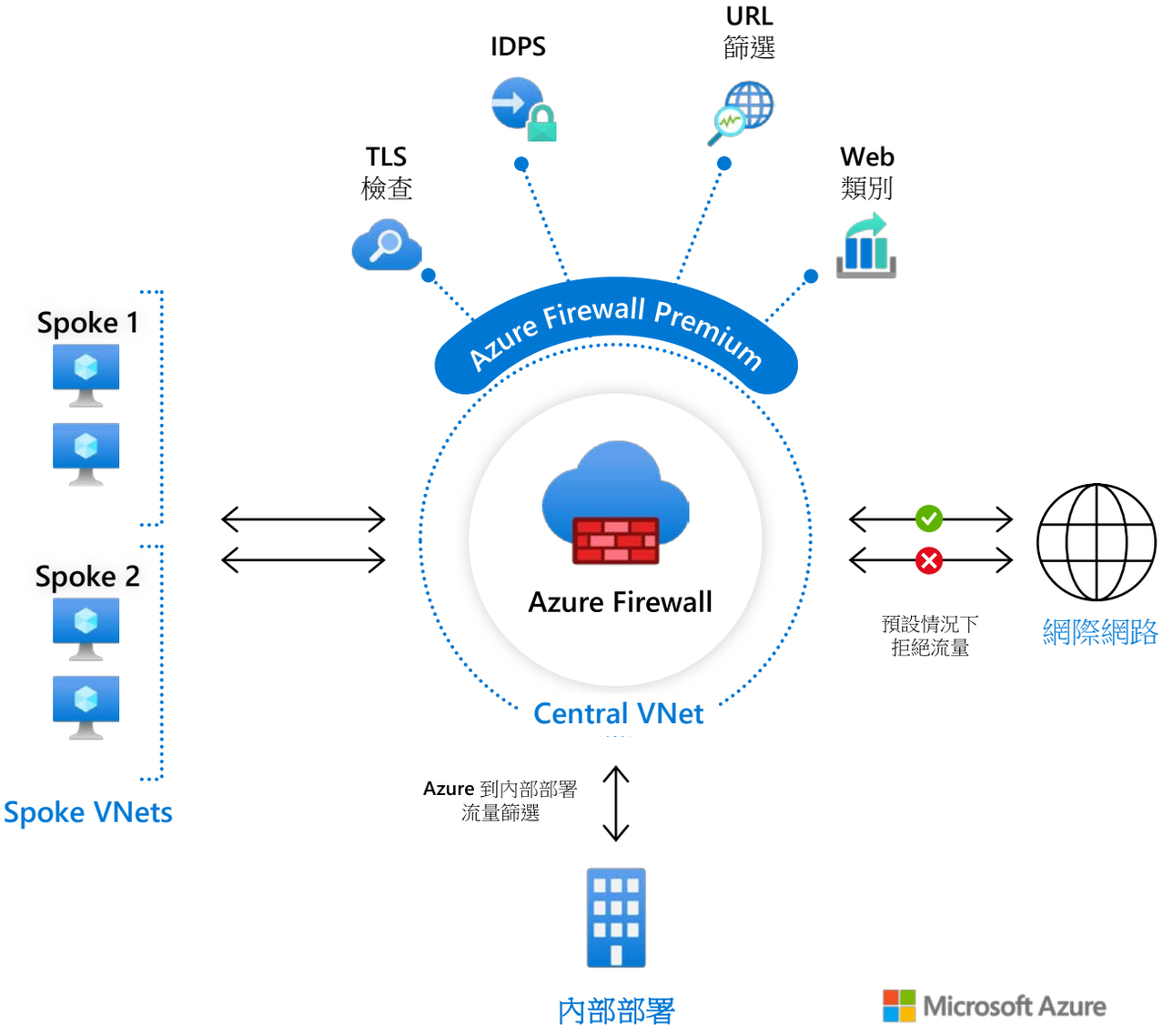
允許或拒絕使用者存取網站類別，如賭博、社交媒體等

保持並持續更新 Web 類別

基於 URL 的類別匹配

Azure 防火牆標準

包括所有標準防火牆功能



使用 Azure 防火牆保護 Azure 虛擬桌面