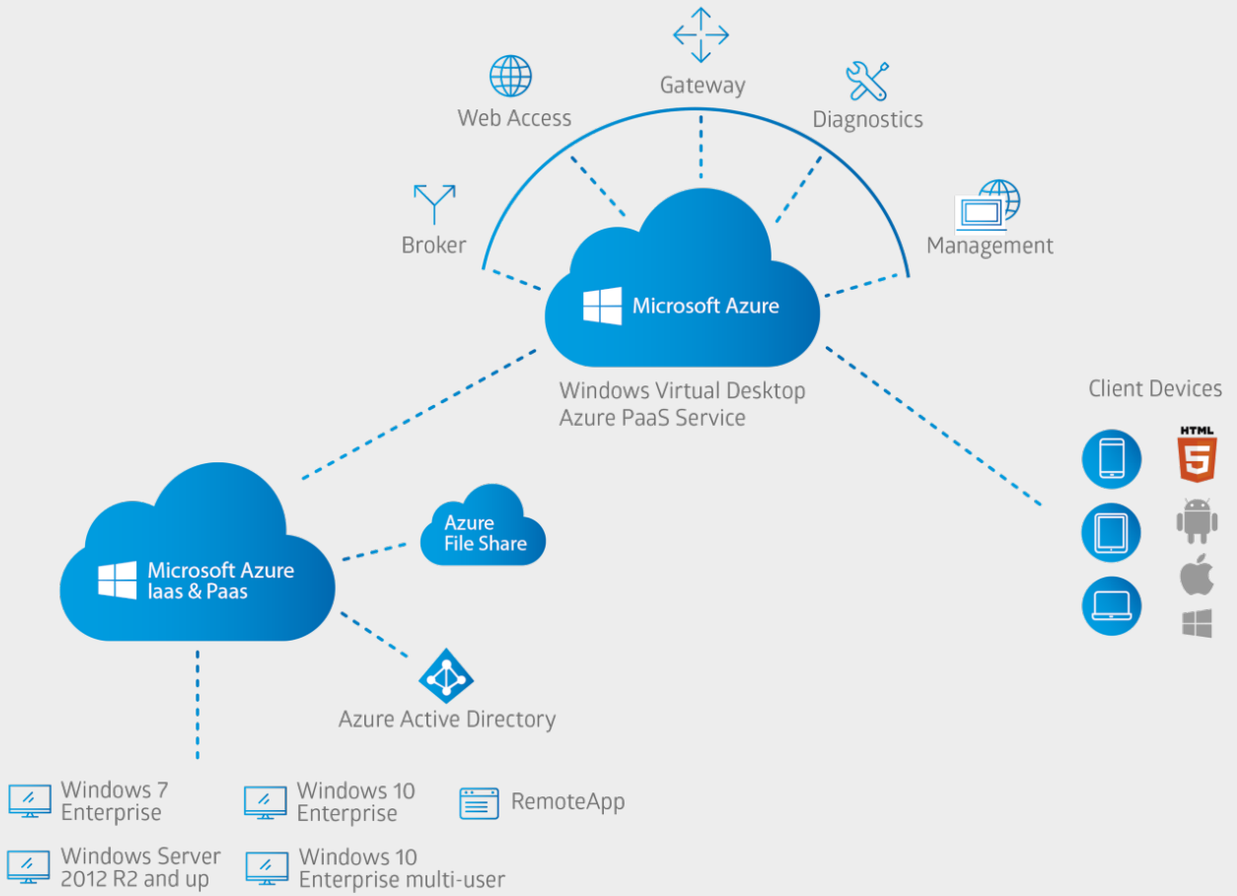
Microsoft Azure

Azure Virtual Desktop Protection

AVD Protection – Solution Pitch Deck and Architecture

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

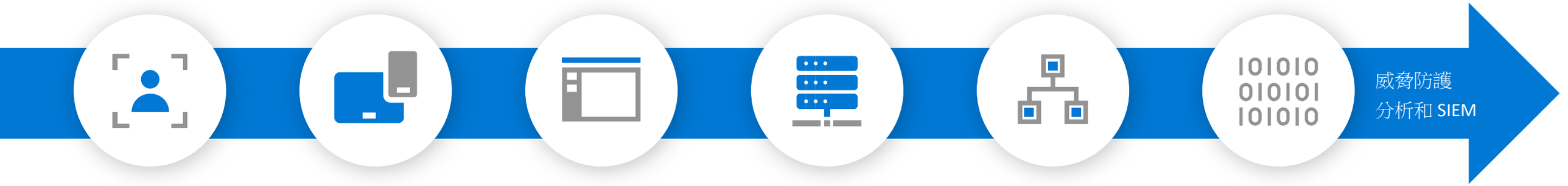
單一平台同時滿足 RDS/VDI 應用情境

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

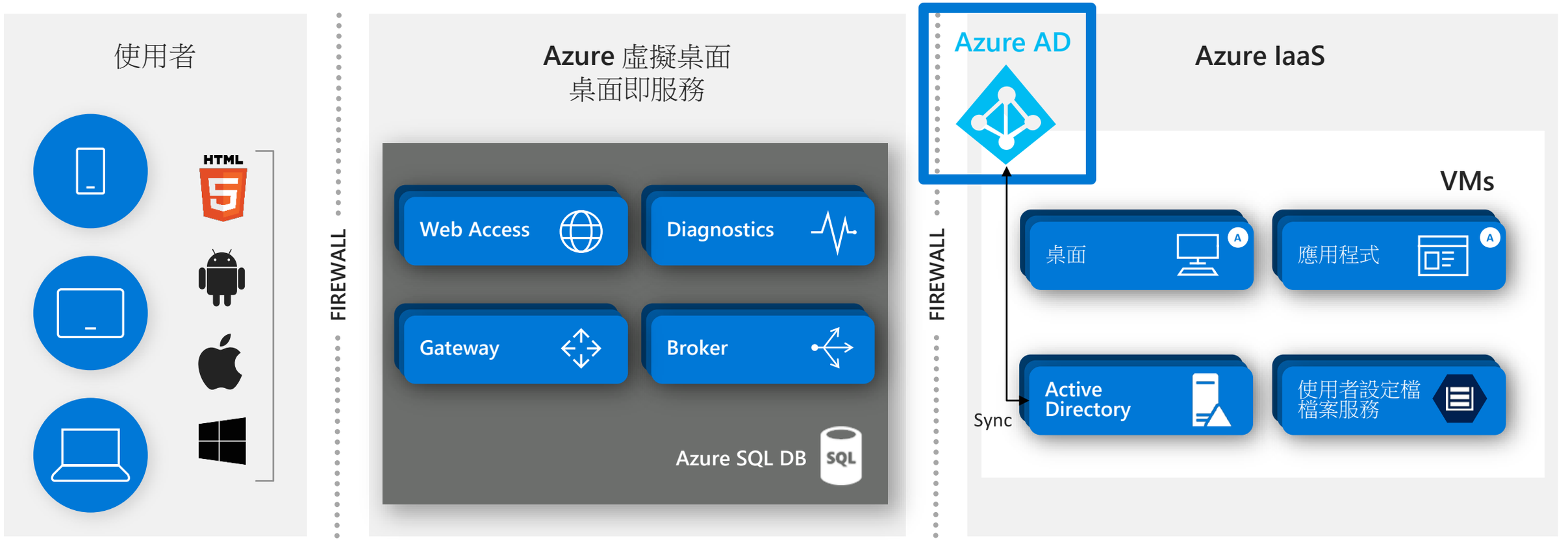
身分識別

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

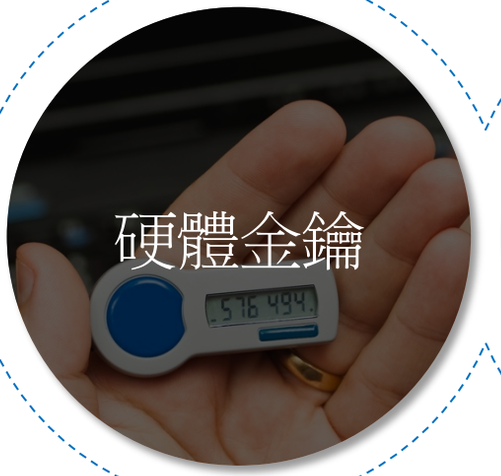
Azure AD 身份保護提供有風險的登入和使用者報告，可與條件式存取一起使用



身分識別 – MFA

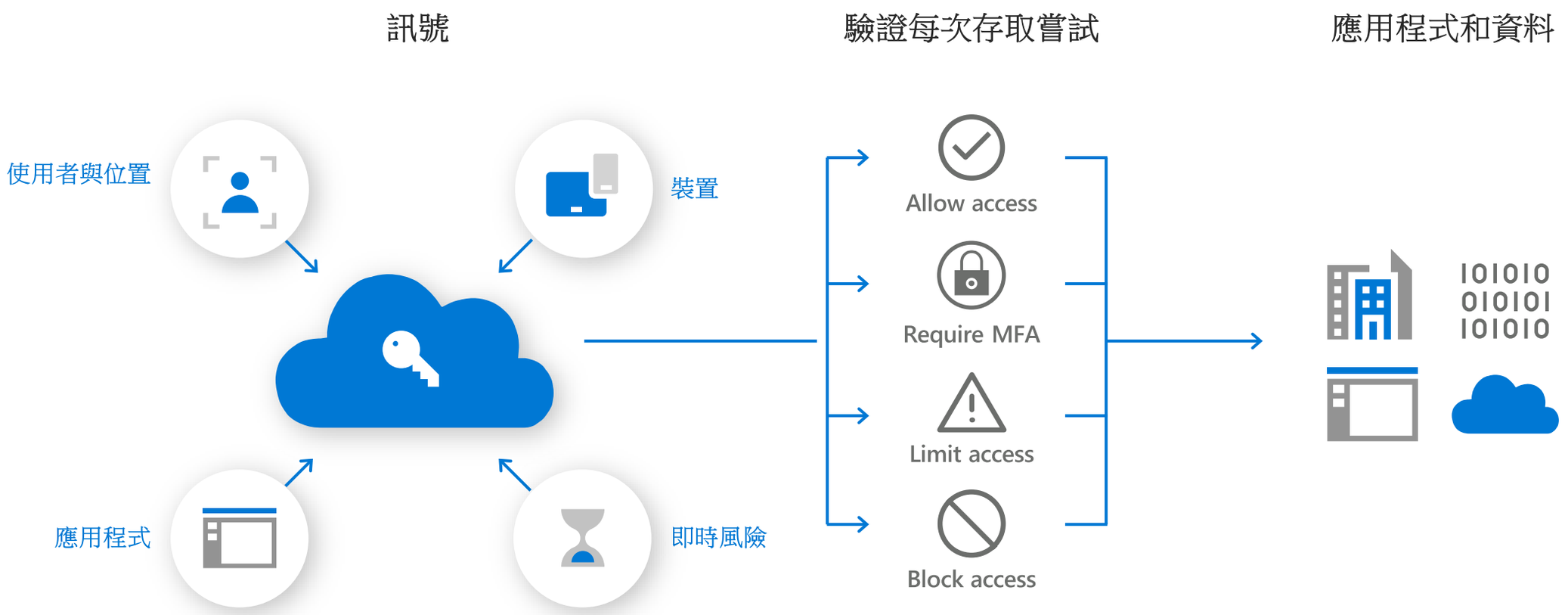
使用多重要素驗證驗證使用者

多因素身份驗證可防止 99.9% 的身份攻擊



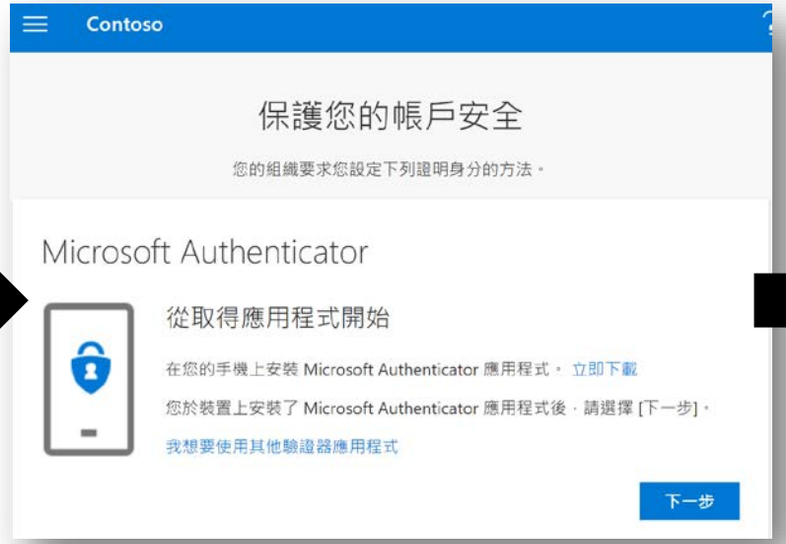
身分識別 – 條件式存取

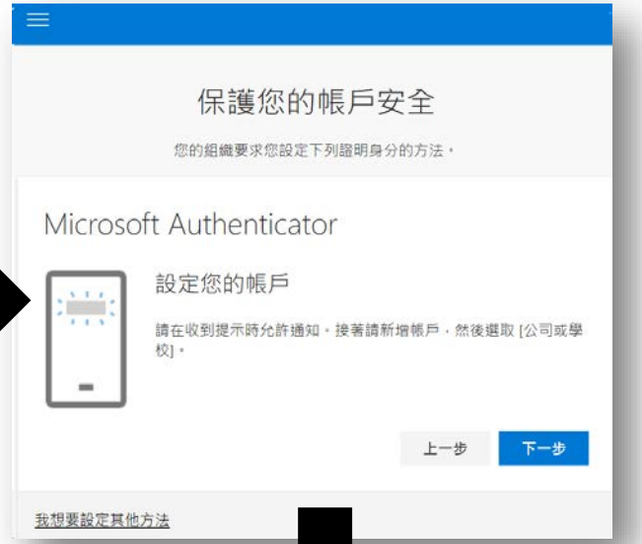
實施強有力的保護原則和風險評估

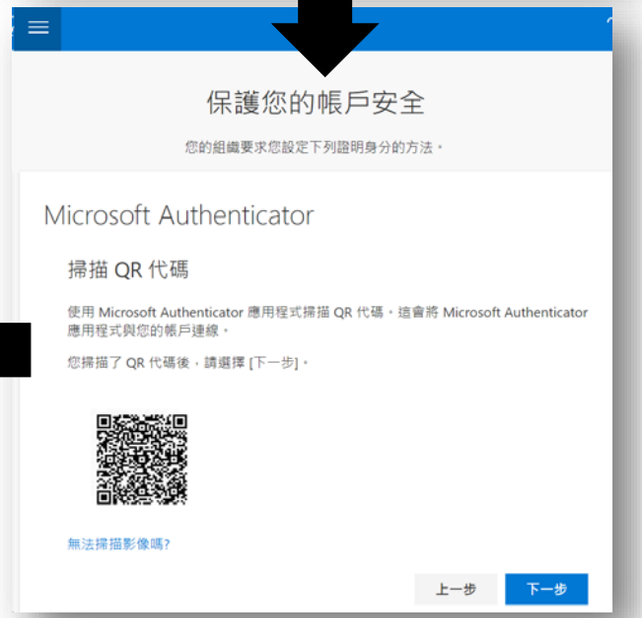


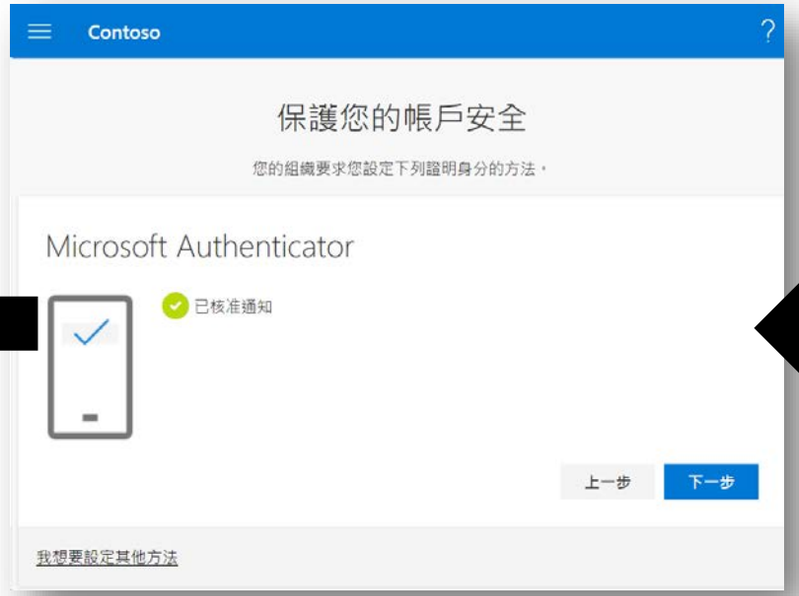
使用者註冊 MFA

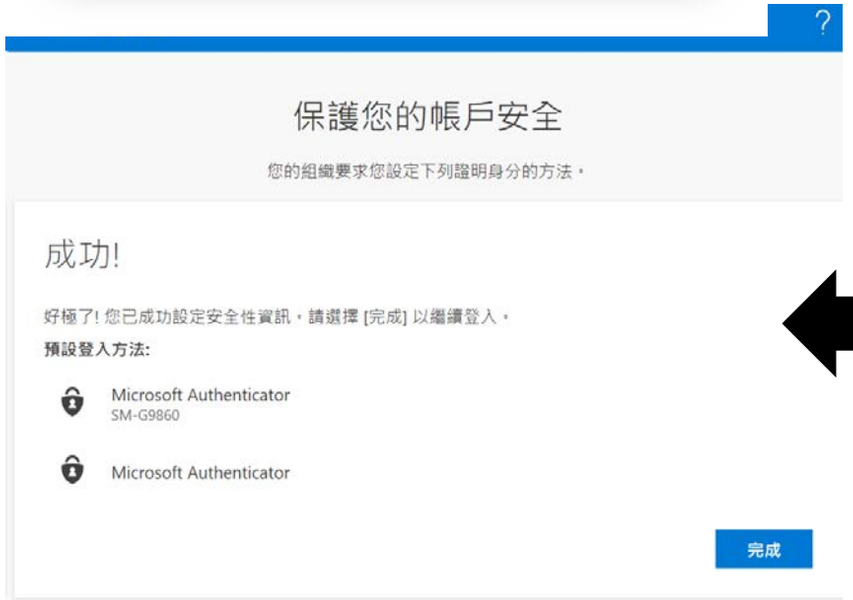

Microsoft
user@contoso.com
需要更多資訊
您的組織需要更多資訊，才能保護您帳戶的安全
使用其他帳戶
進一步了解
下一步


Contoso
保護您的帳戶安全
您的組織要求您設定下列證明身分的方法。
Microsoft Authenticator
從取得應用程式開始
在您的手機上安裝 Microsoft Authenticator 應用程式。 立即下載
您於裝置上安裝了 Microsoft Authenticator 應用程式後，請選擇 [下一步]。
我想要使用其他驗證器應用程式
下一步


保護您的帳戶安全
您的組織要求您設定下列證明身分的方法。
Microsoft Authenticator
設定您的帳戶
請在收到提示時允許通知。接著請新增帳戶，然後選取 [公司或學校]。
上一步
下一步
我想要設定其他方法

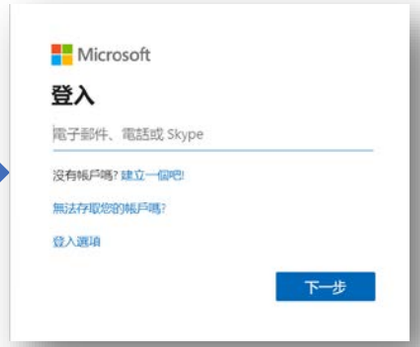

保護您的帳戶安全
您的組織要求您設定下列證明身分的方法。
Microsoft Authenticator
掃描 QR 代碼
使用 Microsoft Authenticator 應用程式掃描 QR 代碼。這會將 Microsoft Authenticator 應用程式與您的帳戶連線。
您掃描了 QR 代碼後，請選擇 [下一步]。
無法掃描影像嗎?
上一步
下一步


Contoso
保護您的帳戶安全
您的組織要求您設定下列證明身分的方法。
Microsoft Authenticator
已核准通知
上一步
下一步
我想要設定其他方法


保護您的帳戶安全
您的組織要求您設定下列證明身分的方法。
成功!
好極了! 您已成功設定安全性資訊。請選擇 [完成] 以繼續登入。
預設登入方法:
Microsoft Authenticator
SM-G9860
Microsoft Authenticator
完成

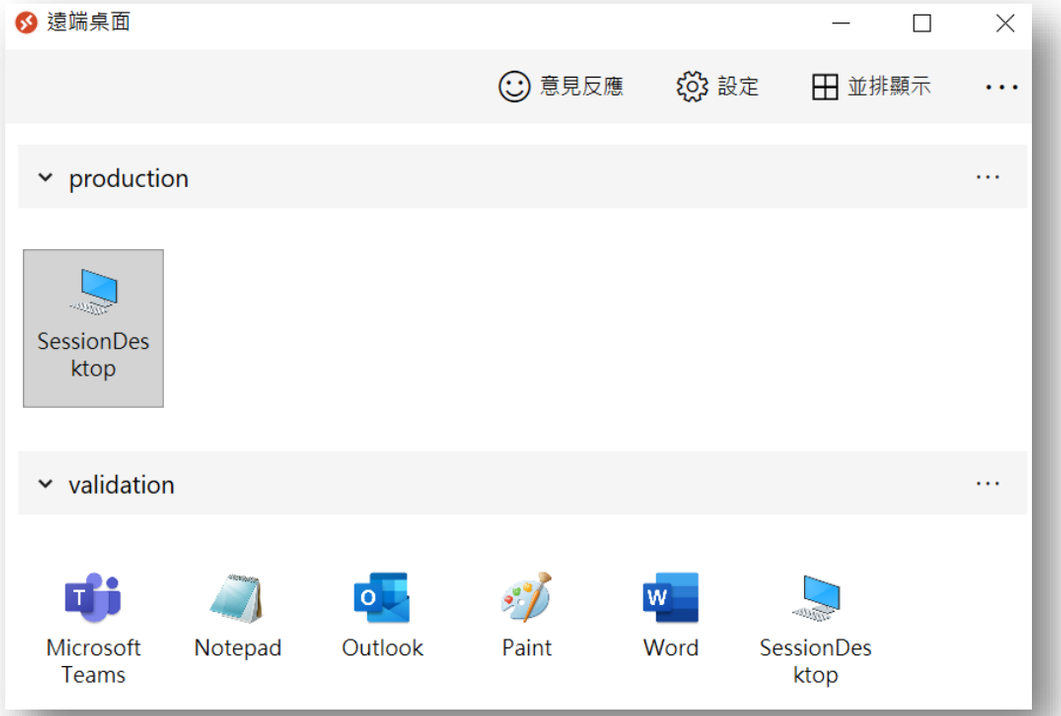
使用者登入 AVD


遠端桌面
意見反應
設定
並排顯示
讓我們開始吧
訂閱您組織所提供的存取受管理的應用程式和桌上型電腦。這些資源可在此用戶端及 [開始功能表] 中取得。
您的組織已預先設定受管理資源的隱私權設定。深入了解
訂閱
用 URL 訂閱


Microsoft
登入
電子郵件、電話或 Skype
沒有帳戶嗎? 建立一個吧!
無法存取您的帳戶嗎?
登入選項
下一步


Microsoft
user@contoso.com
核准登入要求
開啟您的 Microsoft Authenticator 應用程式，並核准登入的要求。
出現問題嗎? 請以另一種方法登入


要核准登入嗎?
Contoso
user@contoso.com
拒絕
核准


遠端桌面
意見反應
設定
並排顯示
production
SessionDesktop
validation
Microsoft Teams
Notepad
Outlook
Paint
Word
SessionDesktop

作業系統

Microsoft Defender for EndPoint

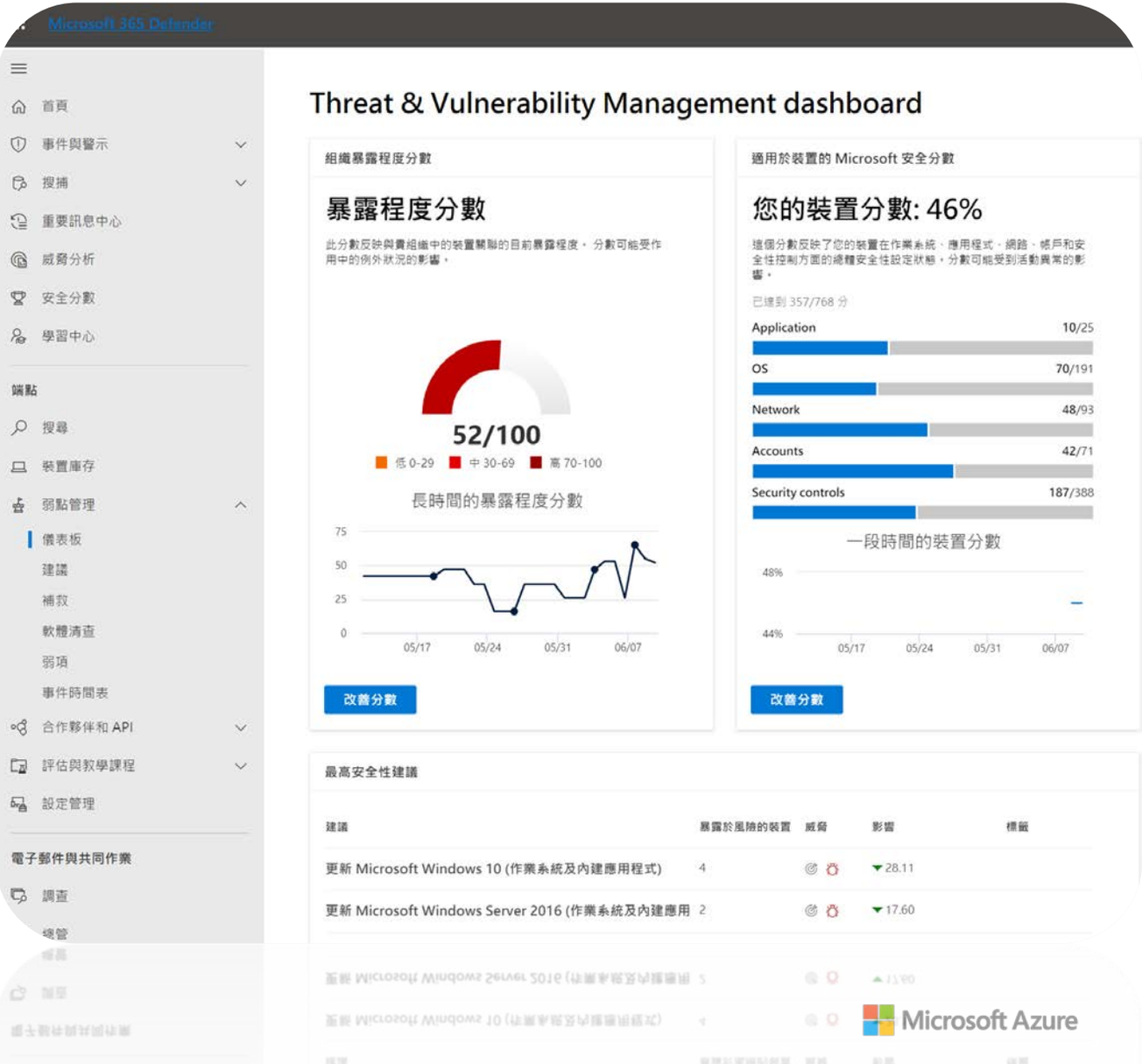
適用於端點的 Microsoft Defender

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



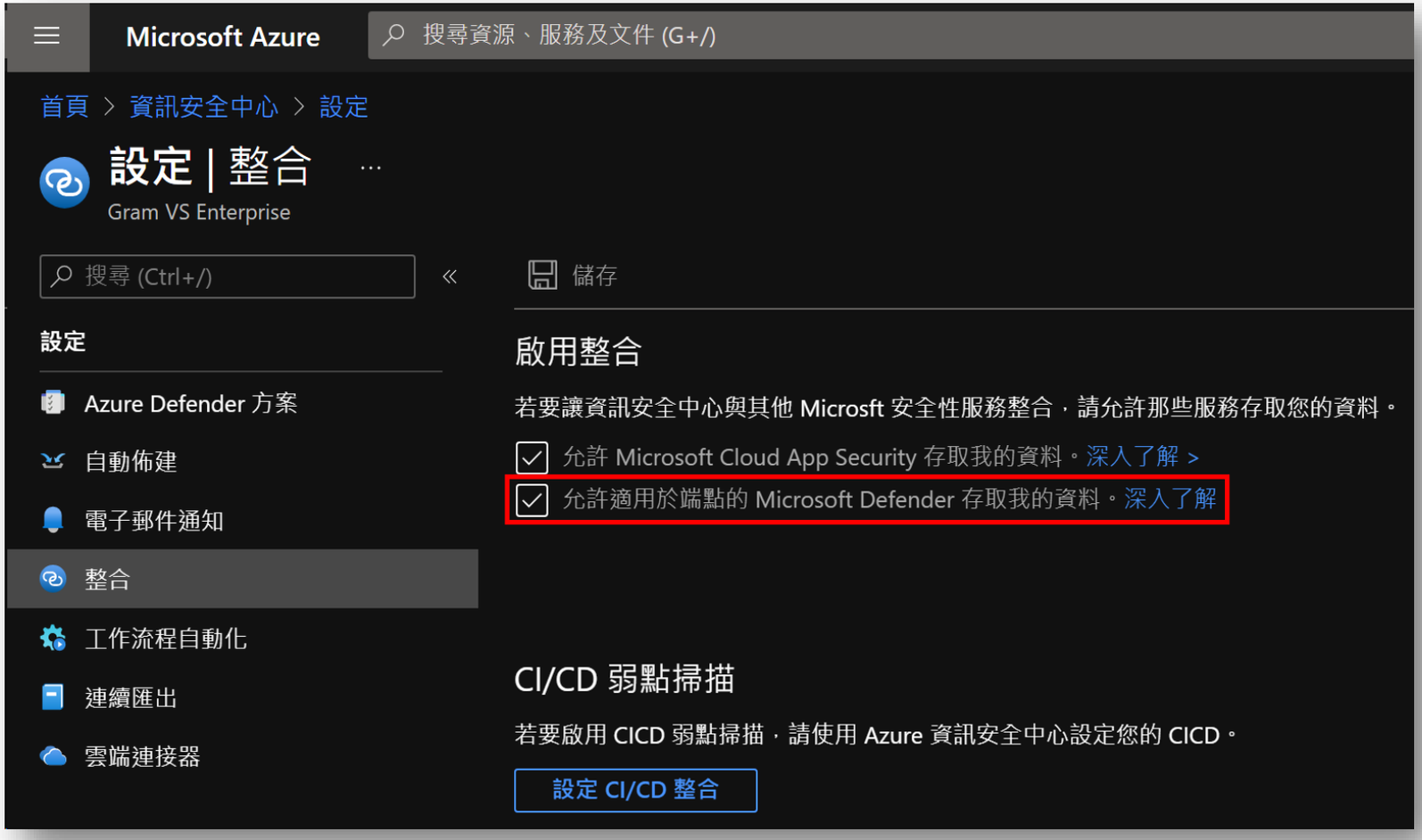
啟用 Azure Defender 整合

啟用適用於伺服器的 Azure Defender

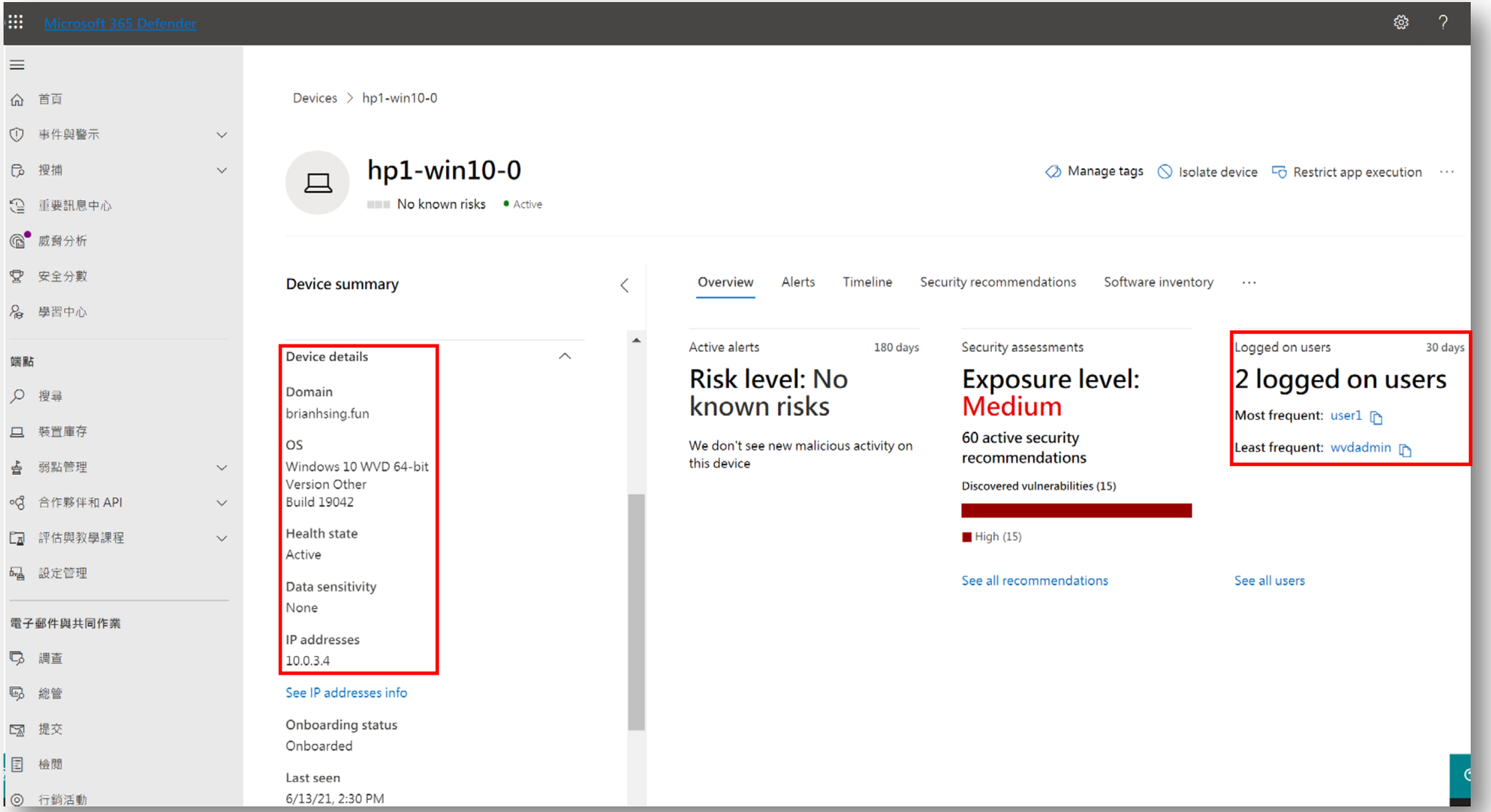
MicrosoftMonitoringAgent 為必要

安全性系統管理員、擁有者

自動上線



裝置詳細資料


Microsoft 365 Defender
首頁
事件與警示
搜捕
重要訊息中心
威脅分析
安全分數
學習中心
端點
搜尋
裝置庫存
弱點管理
合作夥伴和 API
評估與教學課程
設定管理
電子郵件與共同作業
調查
總管
提交
檢閱
行銷活動
Devices > hp1-win10-0
hp1-win10-0
No known risks
Active
Manage tags
Isolate device
Restrict app execution
Device summary
Device details
Domain
brianhsing.fun
OS
Windows 10 WVD 64-bit
Version Other
Build 19042
Health state
Active
Data sensitivity
None
IP addresses
10.0.3.4
See IP addresses info
Onboarding status
Onboarded
Last seen
6/13/21, 2:30 PM
Overview
Alerts
Timeline
Security recommendations
Software inventory
Active alerts
180 days
Risk level: No known risks
We don't see new malicious activity on this device
Security assessments
Exposure level: Medium
60 active security recommendations
Discovered vulnerabilities (15)
High (15)
See all recommendations
Logged on users
30 days
2 logged on users
Most frequent: user1
Least frequent: wvdadmin
See all users

作業系統 – 安全性考量

持續更新定義企業原則

修補軟體漏洞

使用最新的作業系統更新主機或重新部署

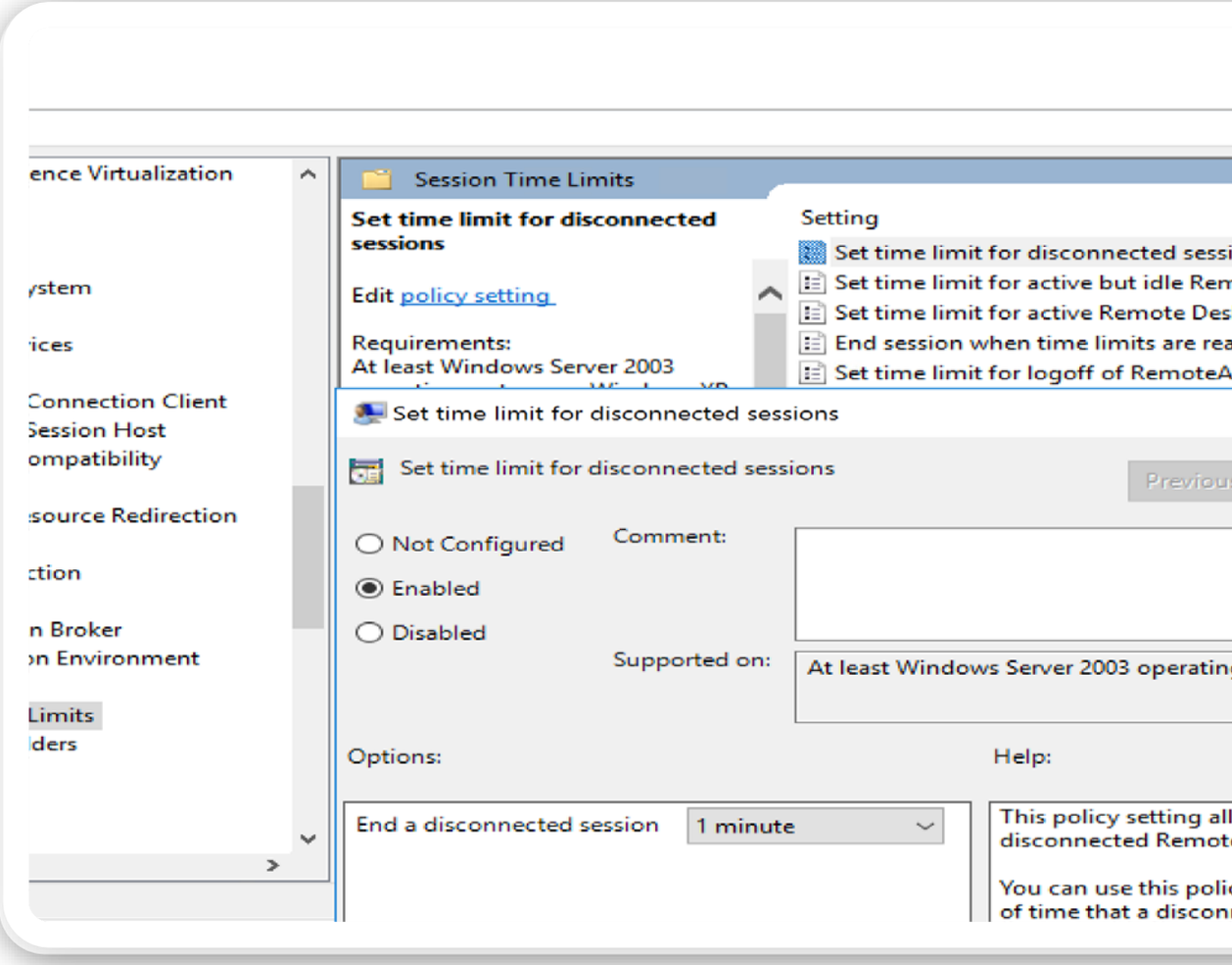
控制裝置重新導向

預設禁用智慧卡、連接埠、硬體、視訊重新導向

定義群組原則

設定使用者閒置時間限制

設定使用者斷線時間限制



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

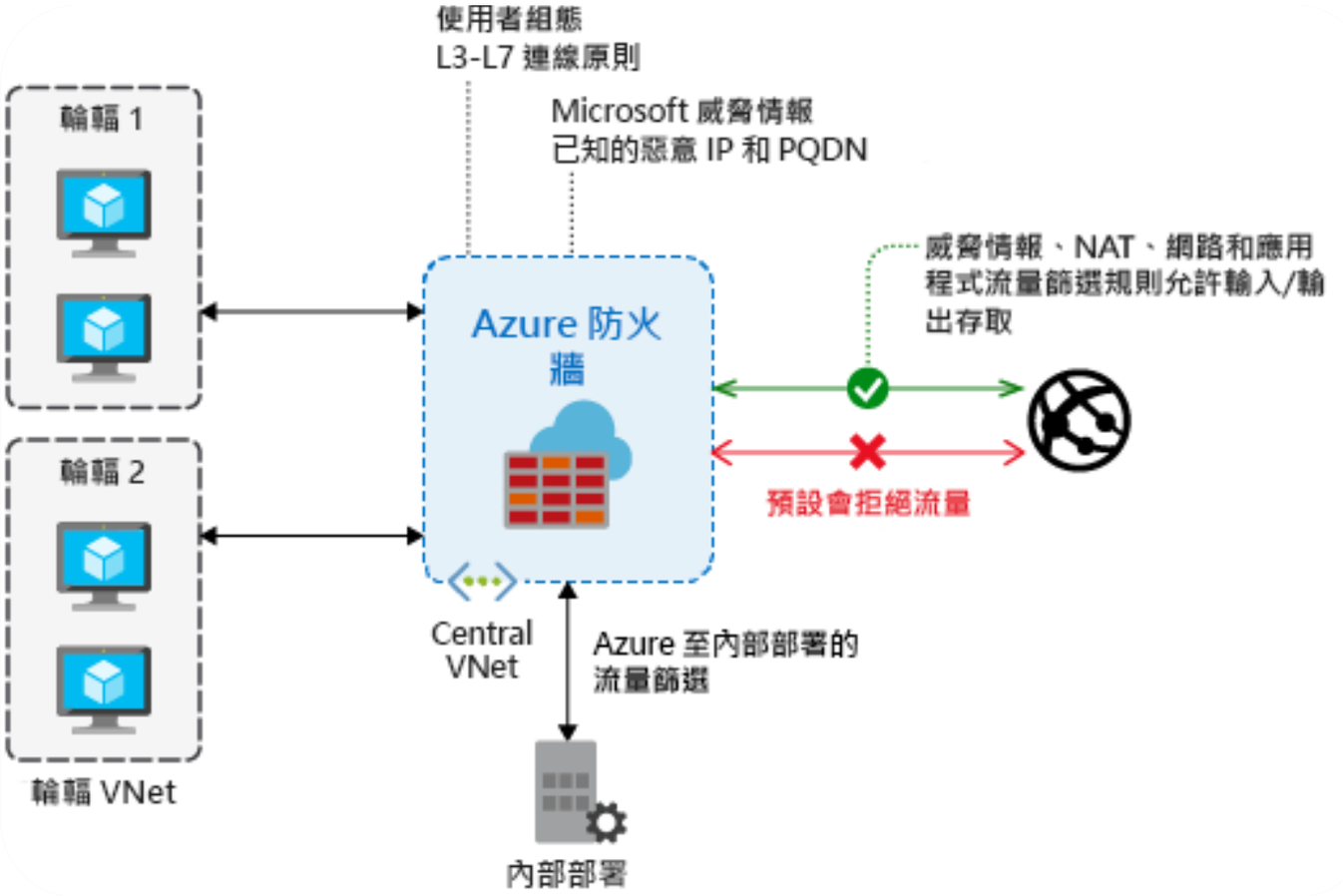
跨 VNet 和訂閱的集中原則

完整的 VNET 保護

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

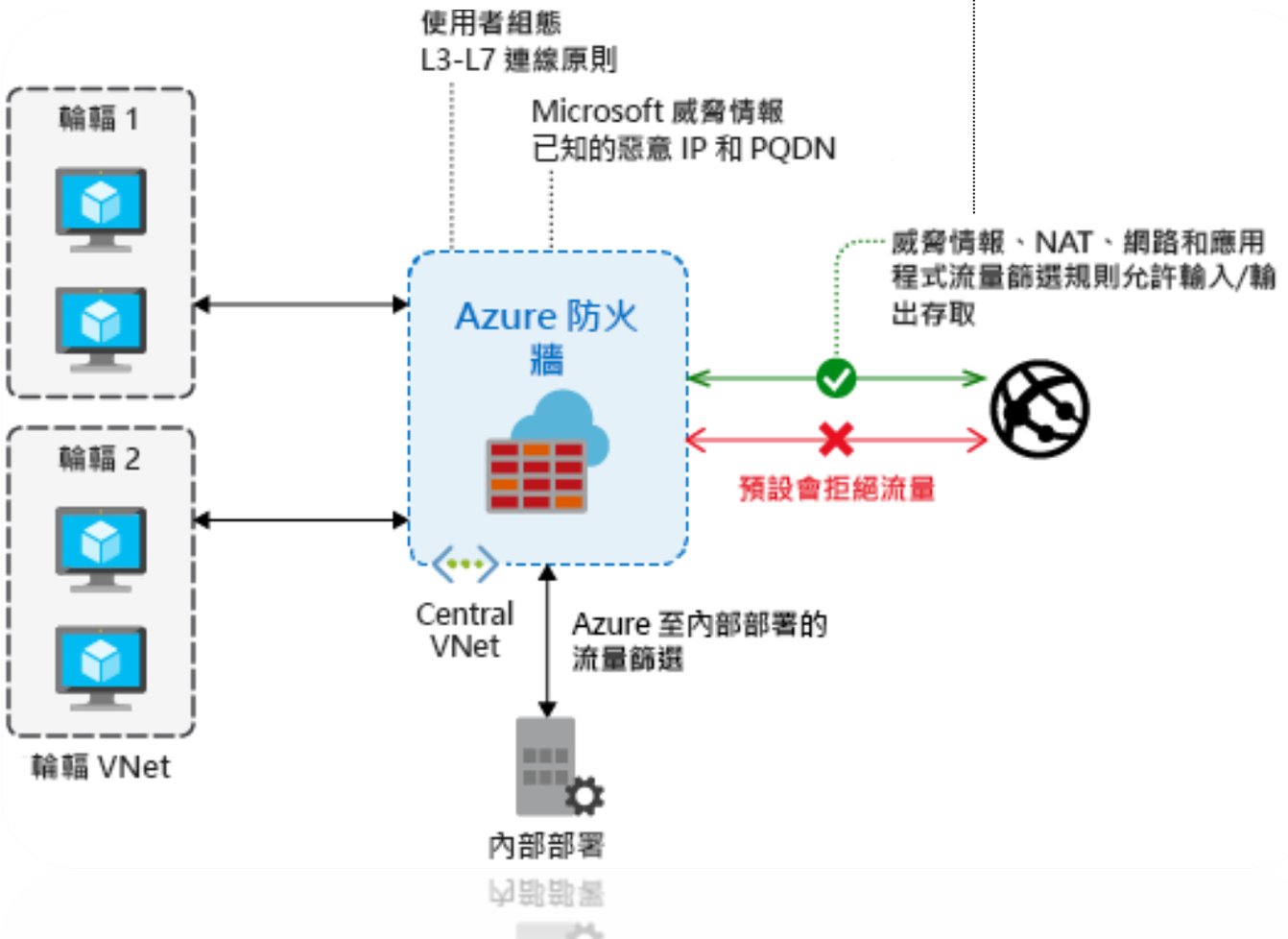
集中式記錄

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**

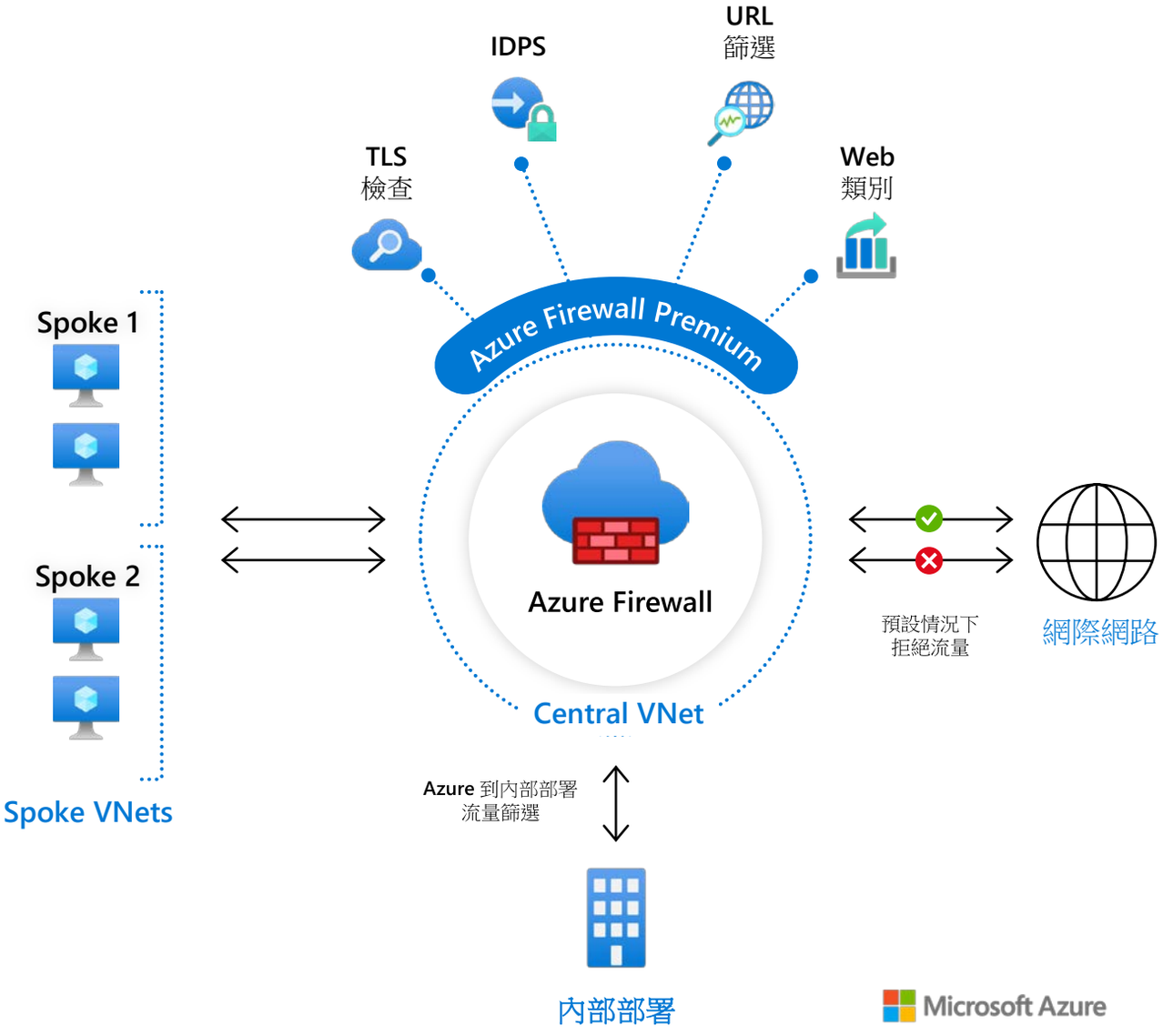
允許或拒絕使用者存取網站類別，如賭博、社交媒體等

保持並持續更新 Web 類別

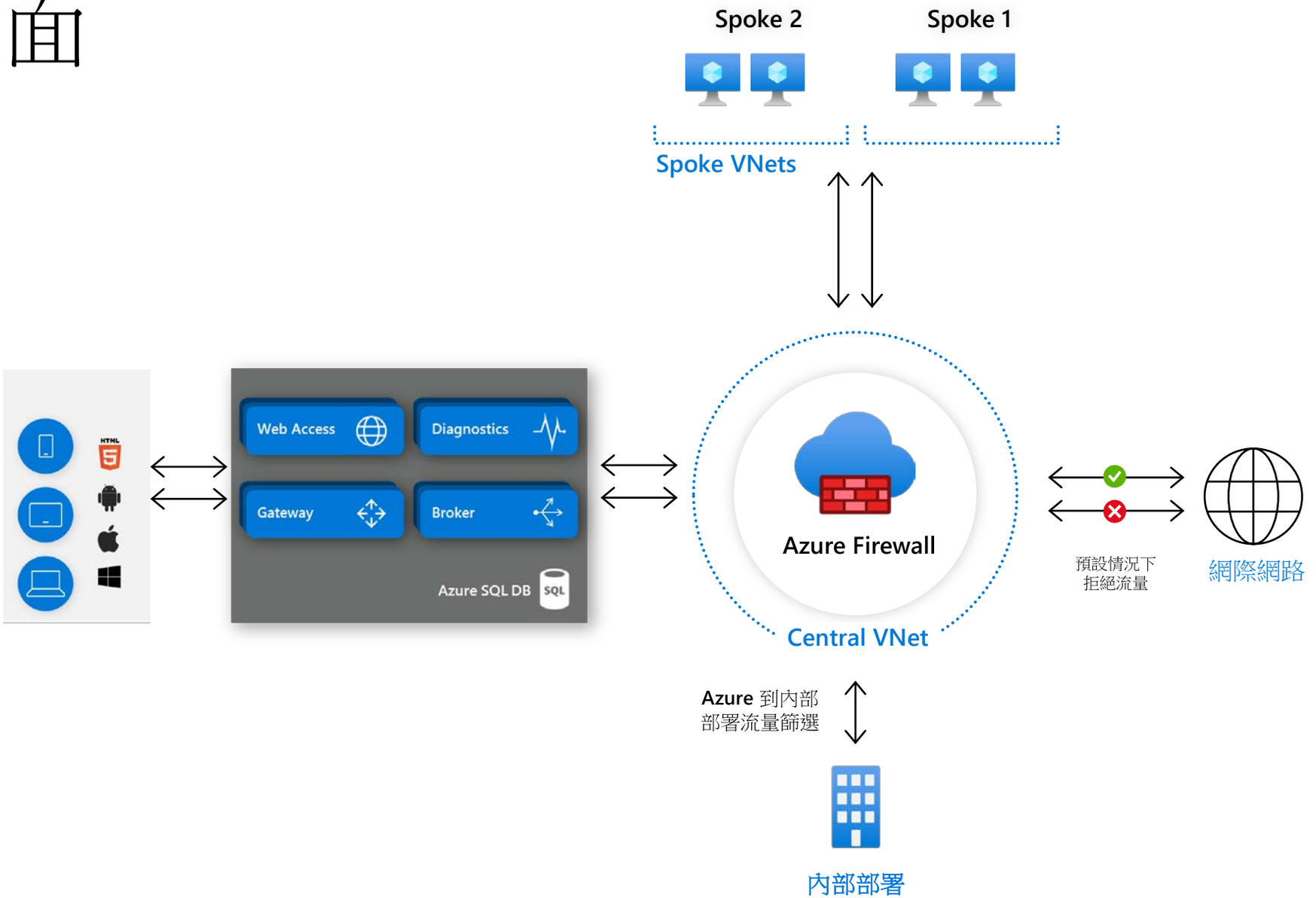
基於 URL 的類別匹配

Azure 防火牆標準

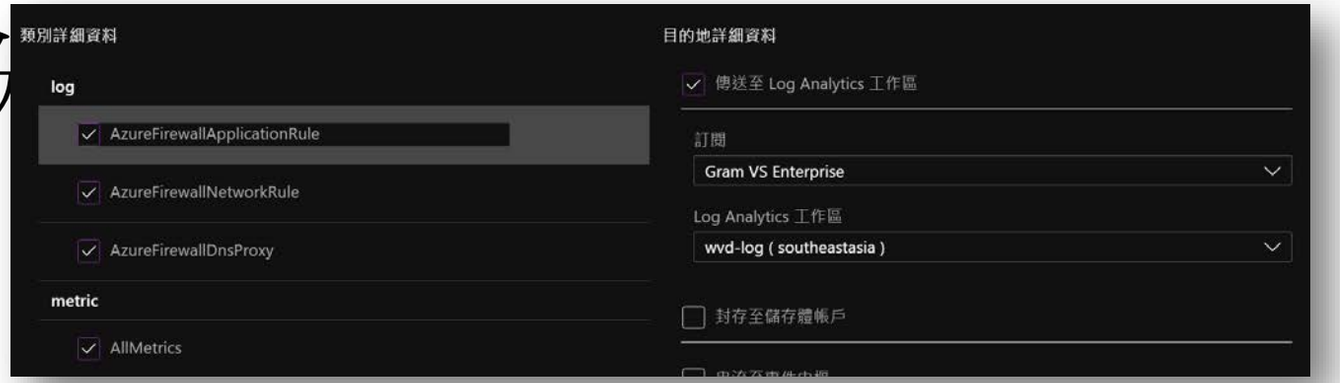
包括所有標準防火牆功能



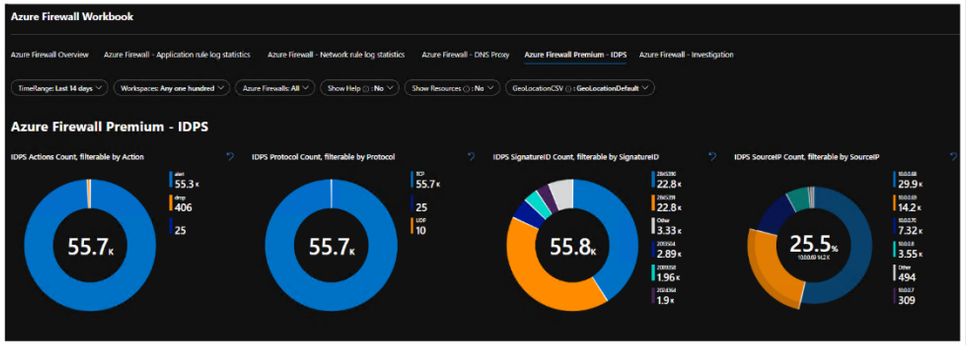
如何使用 Azure 防火牆保護 Azure 虛擬桌面



Azure 防火牆日誌分



Azure Monitor Workbook for Azure Firewall



Gain insights into Azure Firewall events. You can learn about your application and network rules, see statistics for firewall activities across URLs, ports, and addresses. This workbook allows you to filter your Firewalls and Resource Groups, dynamically filter per category with easy to read data sets when investigating an issue in your logs. Import via ARM Template or Gallery Template.

Deploy to Azure

When deploying via ARM Template, please make sure you know what Resource ID (Log Analytics Workgroup) you're wanting to use.

> Example of a value: /subscriptions/'GUID'/resourcegroups/'RG Name'/providers/microsoft.operationalinsights/workspaces/'Workspace Name'

This workbook visualizes security-relevant Azure Firewall events across several filterable panels for Mutli-Tenant/Workspace view. It works with all Azure Firewall data types, including Application Rule Logs, Network Rule Logs, DNS Proxy logs and ThreatIntel logs. Import via ARM Template or Gallery Template.

All IP addresses events: Query Time(922毫秒) : Total Rows(148)

搜尋

TimeGenerated	FQDN	Protocol	Action	SourceIP	SourcePort	Dest...	ResourceId	ResourceGroup
2021/6/13 下午8:43:16	aefd.nelreports.net	HTTPS	Deny	10.0.3.4	55699	443	AZFW	AZFW-RG
2021/6/13 下午8:43:16	deff.nelreports.net	HTTPS	Deny	10.0.3.4	62564	443	AZFW	AZFW-RG
2021/6/13 下午8:43:17	aefd.nelreports.net	HTTPS	Deny	10.0.3.4	55105	443	AZFW	AZFW-RG
2021/6/13 下午8:43:17	deff.nelreports.net	HTTPS	Deny	10.0.3.4	56811	443	AZFW	AZFW-RG
2021/6/13 下午8:43:17	deff.nelreports.net	HTTPS	Deny	10.0.3.4	54948	443	AZFW	AZFW-RG
2021/6/13 下午8:43:32	edge.microsoft.com	HTTPS	Deny	10.0.3.4	53646	443	AZFW	AZFW-RG
2021/6/13 下午8:43:33	edge.microsoft.com	HTTPS	Deny	10.0.3.4	58549	443	AZFW	AZFW-RG
2021/6/13 下午8:43:54	www.bing.com	HTTPS	Deny	10.0.3.4	52474	443	AZFW	AZFW-RG
2021/6/13 下午8:42:01	config.edge.skype.com	HTTPS	Deny	10.0.3.4	51876	443	AZFW	AZFW-RG
2021/6/13 下午8:42:11	www.bing.com	HTTPS	Deny	10.0.3.4	54947	443	AZFW	AZFW-RG
2021/6/13 下午8:42:14	www.bing.com	HTTPS	Deny	10.0.3.4	64655	443	AZFW	AZFW-RG

https://github.com/Azure/Azure-Network-Security/tree/master/Azure%20Firewall/Workbook%20-%20Azure%20Firewall%20Monitor%20Workbook