

Using Azure Protect Web – Solution Pitch Deck and Architecture

Web 應用程式 攻擊現況



DDoS 攻擊

蠻力攻擊用以癱瘓網路連結與資源

攻擊範例

TCP Syn Flood, UDP Reflection, Amplification, Http(s) flood



網頁應用程式攻擊

利用 web 應用程式漏洞

攻擊範例

OWASP TOP 10: SQL injection, Cross Site Scripting, OS command injection, Remote File Inclusion



惡意機器人

同時以基礎設施與網頁應用程式為目標，用於在競爭者中取得優勢

攻擊範例

網頁內容與價格爬蟲, 憑證填充 (credential stuffing)

Key Security Areas

識別與存取

- 保護應用程式存取權限

網路安全

- 存取控制, 隔離(isolation)

資料安全與加密

- 靜態加密, 運行中加密和密鑰管理

系統整合

- 修補、強化、權限分配

見解 (Insights)

- 評估Azure資源的安全狀態以辨識潛在的安全漏洞

應用程式安全

- 避免程式漏洞

利用 Azure 服務簡化安全管理



Identity & access management

Azure Active Directory

Multi-Factor Authentication

Role Based Access Control

Azure Active Directory (Identity Protection)



Data protection

Encryption (Disks, Storage, SQL)

Azure Key Vault



Network security

VNET, VPN, NSG

Application Gateway (WAF), Azure Firewall

DDoS Protection Standard

ExpressRoute



Threat protection

Azure Security Center

Microsoft Antimalware for Azure



Security management

Azure Log Analytics

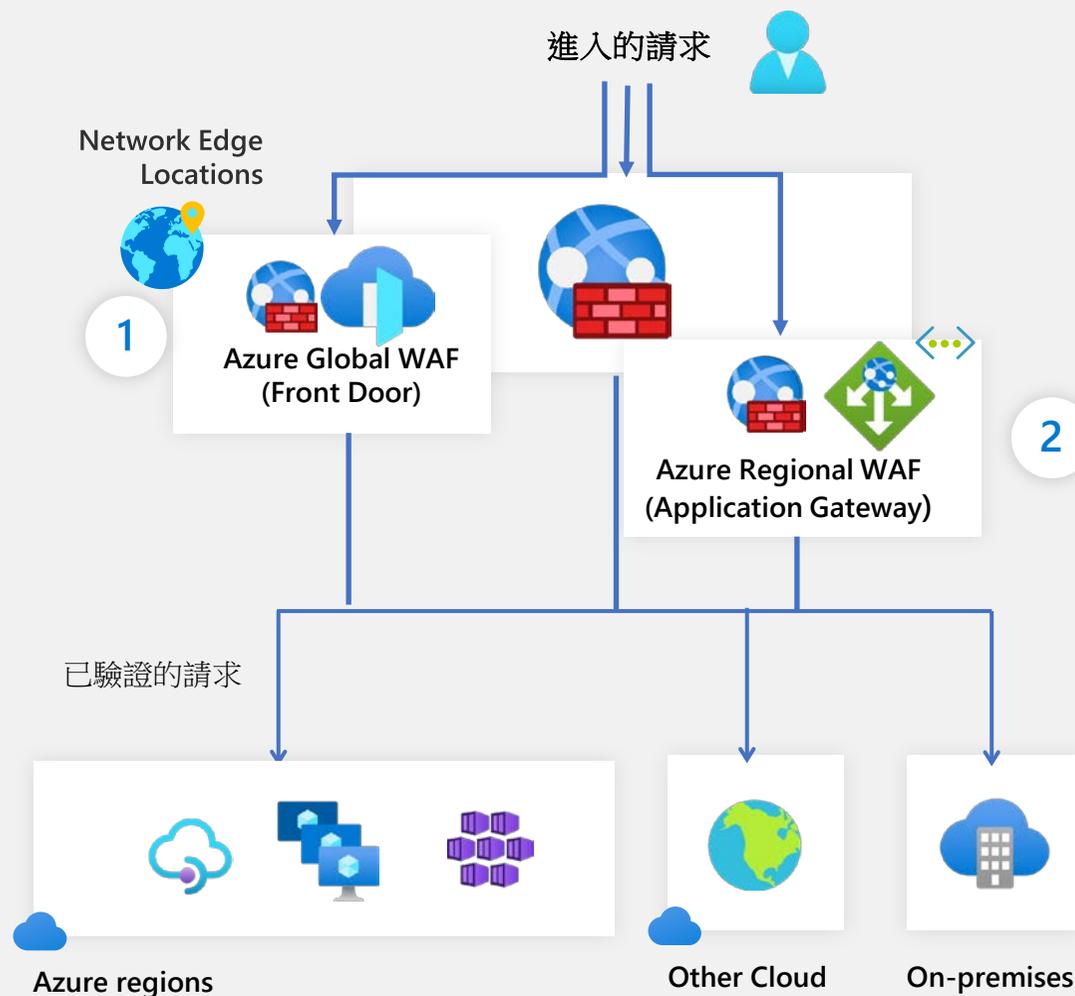
+ Partner Solutions

Azure WAF

保護在 **Azure** 或是任何地方的 **web** 應用程式
受平台託管、易於使用
具高可用性、可擴展性以及高性能
符合企業合規標準

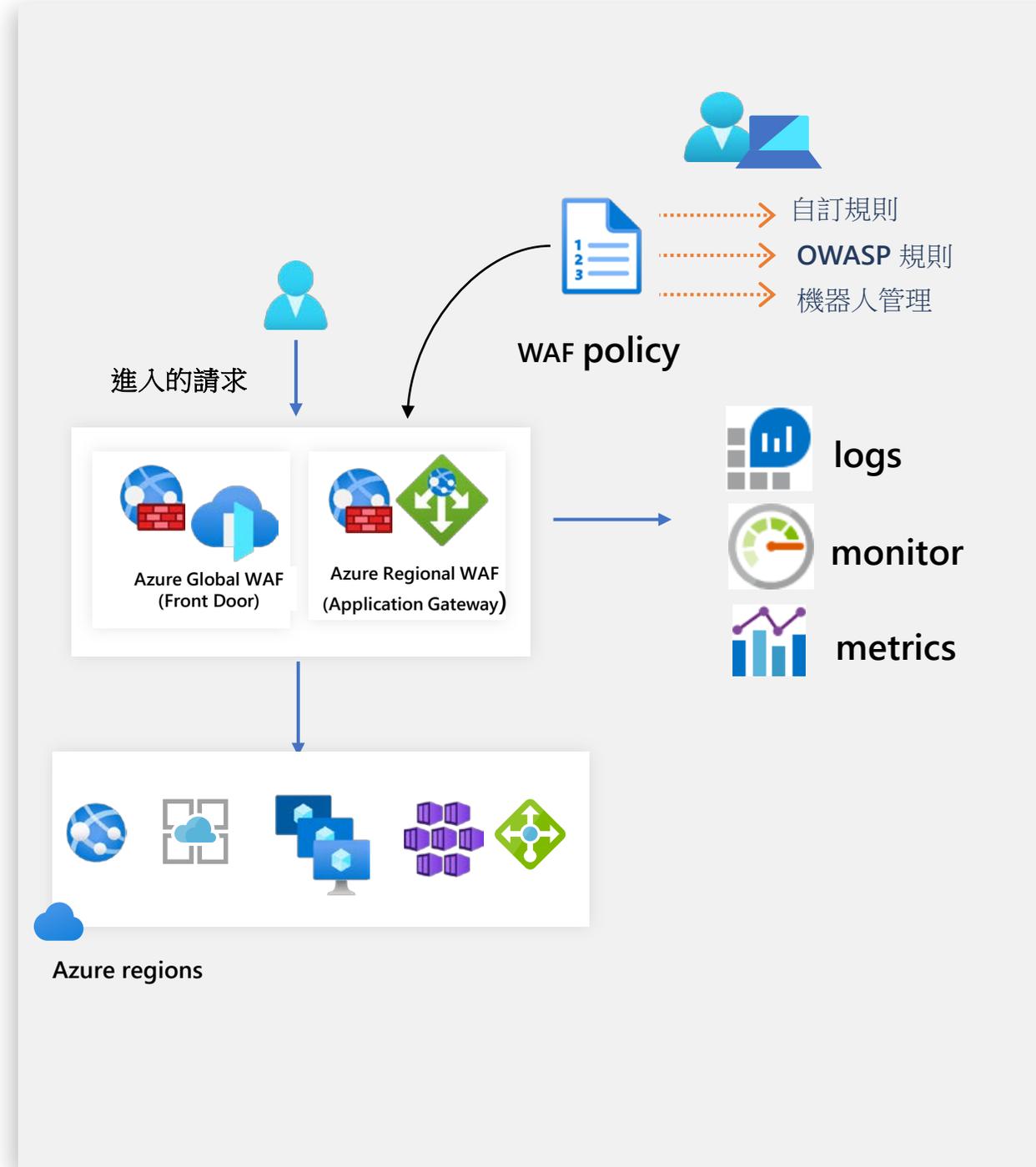
1 與 Azure Front Door 在網路邊緣整合 (network edge)，
結合應用程式加速、快取與保護的功能。

2 與 Application Gateway 整合，保護特定的公開或私人網站



Azure WAF 主要功能

- ✓ 強大的自訂規則引擎
 - Geo-filtering 篩選使用者地區
 - IP restriction 設置 IP 規則
 - http parameters filtering 針對 http 參數過濾
 - size restriction 限制傳送文本大小 (上限更新為 750 MB)
- ✓ 在 **Azure network edge** 設置速率限制條件
- ✓ 預先設置 **OWASP top 10** 攻擊規則 (Rule Set CRS 3.1 added)
- ✓ 與 **Microsoft Threat Intelligence** 整合的機器人保護機制
- ✓ 可與 **Azure Sentinel** 整合
- ✓ 在偵測模式下不產生額外延遲
- ✓ 簡易的設置方式: **Portal, API, PowerShell, Azure CLI, Terraform**



地區篩選



以地理位置來篩選流量

選擇那些國家的流量是允許通過、需封鎖或是需要紀錄的

- 透過減少不必要流量來增進您應用程式的效能
 - 條件邏輯篩選功能增進了對地區篩選的評估
- 可以在 WAF Policy 中輕鬆設置
- 地理資料每周更新

Add custom rule

A custom rule is made up of one or more conditions followed by an action. All custom rules for an Application Gateway WAF policy are match rules.

[Learn more about custom rules](#)

Custom rule name *

Priority *

Conditions

If

Match type

Match variables

Match variable *

+ Add another match variable

Operation

Is Is not

Country code *

+ Add new condition

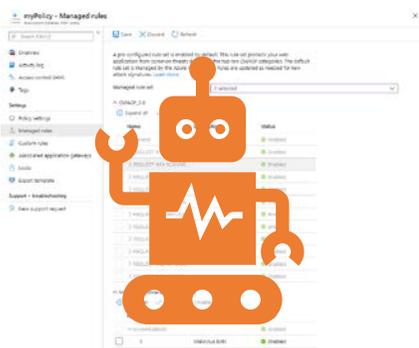
Then

Allow traffic

Deny traffic

Log traffic only

Bot 保護 (Public Preview)



保護您的應用不受到惡意機器人攻擊

Bot 保護受控規則集

- 可與受控 CRS 規則集一起被添加到 WAF 中
- 透過減少不必要流量來增進您應用程式的效能
- 可以在 WAF Policy 中輕鬆設置
- 資料每日更新
(透過 Microsoft threat intelligence)

myPolicy - Managed rules
Application Gateway WAF policy

Search (Ctrl+/)

Save Discard Refresh

A pre-configured rule set is enabled by default. This rule set protects your web application from common threats defined in the top-ten OWASP categories. The default rule set is managed by the Azure WAF service. Rules are updated as needed for new attack signatures. [Learn more](#)

Managed rule set: 2 selected

OWASP_3.0

Expand all Enable Disable

Name	Description	Status
<input type="checkbox"/> > General		Enabled
<input type="checkbox"/> > REQUEST-911-METHO...		Enabled
<input type="checkbox"/> > REQUEST-913-SCANNE...		Enabled
<input type="checkbox"/> > REQUEST-920-PROTOD...		Enabled
<input type="checkbox"/> > REQUEST-921-PROTOD...		Enabled
<input type="checkbox"/> > REQUEST-930-APPLICA...		Enabled
<input type="checkbox"/> > REQUEST-931-APPLICA...		Enabled
<input type="checkbox"/> > REQUEST-932-APPLICA...		Enabled
<input type="checkbox"/> > REQUEST-933-APPLICA...		Enabled
<input type="checkbox"/> > REQUEST-941-APPLICA...		Enabled
<input type="checkbox"/> > REQUEST-942-APPLICA...		Enabled
<input type="checkbox"/> > REQUEST-943-APPLICA...		Enabled

Microsoft_BotManagerRuleSet_0.1

Expand all Enable Disable

Name	Description	Status
<input type="checkbox"/> > KnownBadBots		Enabled
<input type="checkbox"/> 1	Malicious Bots	Enabled

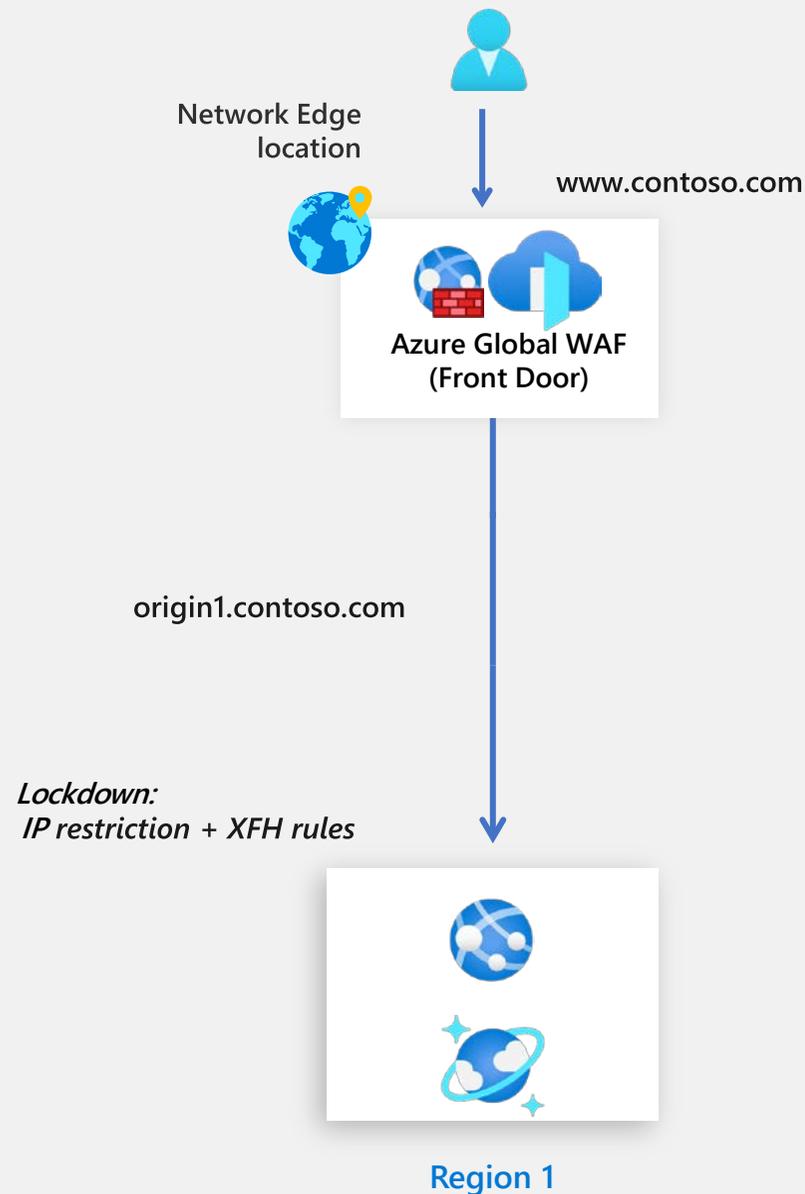
情境 1

WAF 保護裝載於 Azure App Service 上的公開網站

在網路邊緣 (network edge) 透過 Front Door 來啟用 WAF

延遲時間最佳化

鎖定 Web App 只允許來自 Front Door 的流量



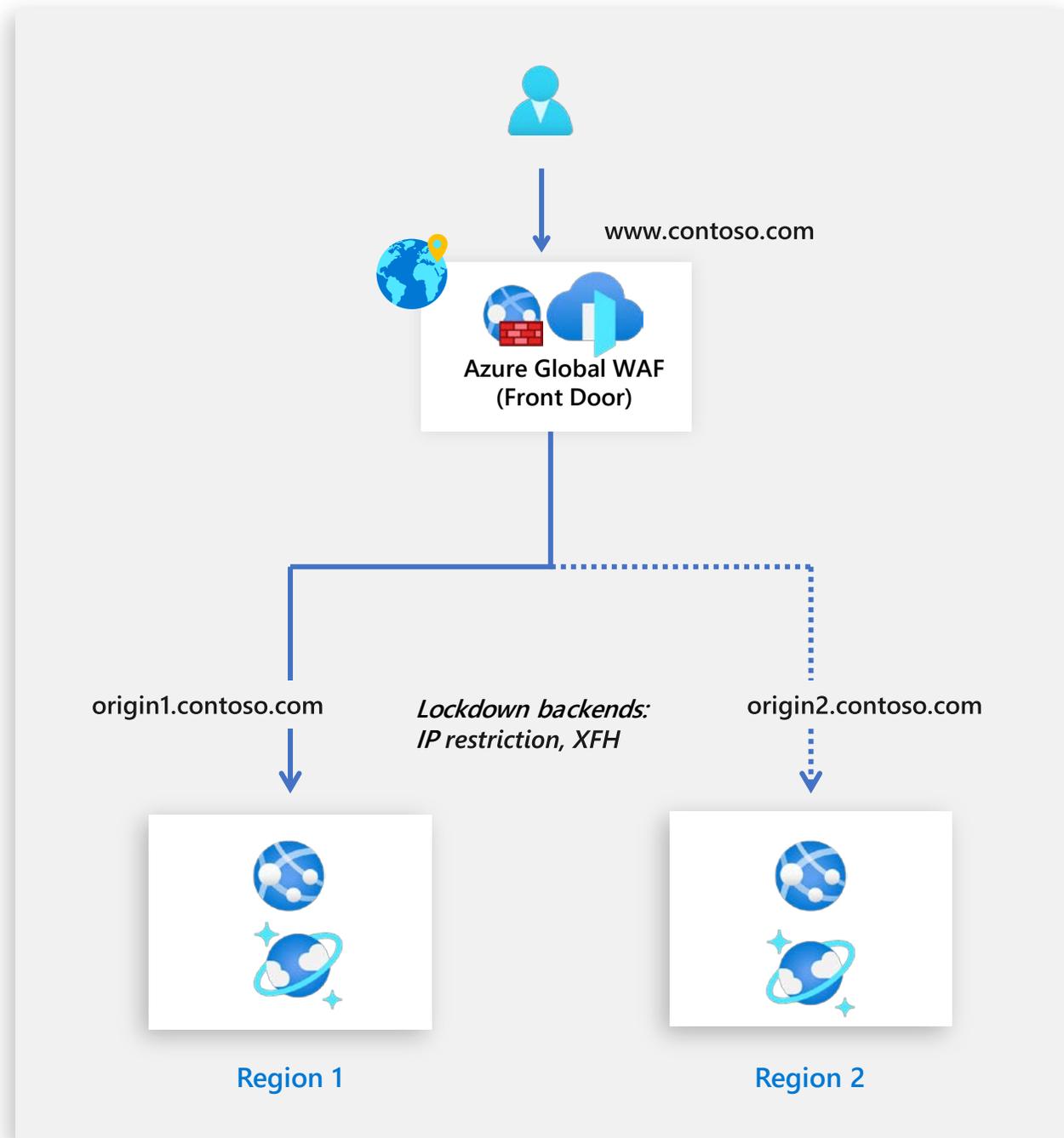
情境 1

WAF 保護裝載於 Azure App Service 上的公開網站

延遲時間最佳化

全球負載平衡

集中的 WAF 政策: 當新增第二個區域 (region) 時不須額外設定



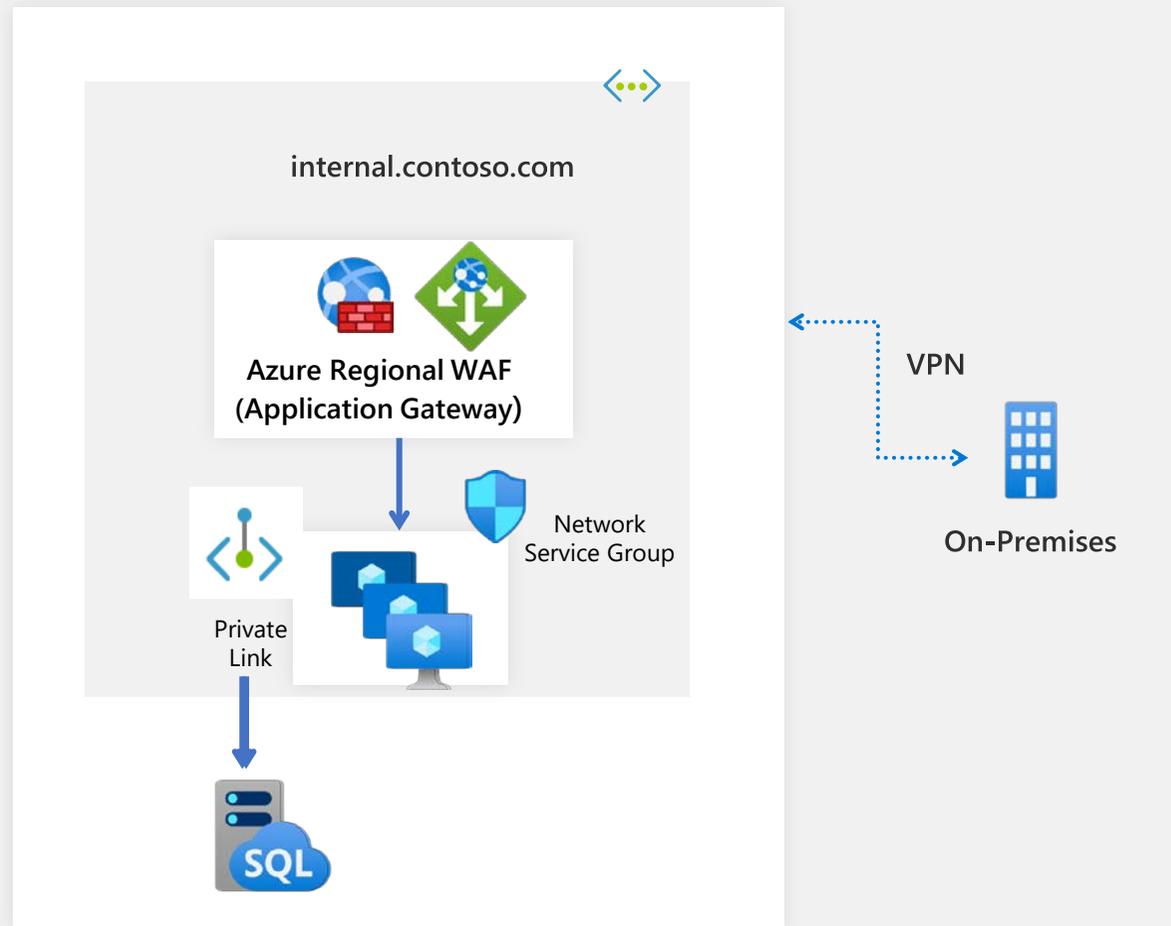
情境 2

WAF 保護在 Vnet 中的私人網站

將特定 WAF 放置於 Vnet 中

在 VMs 間負載平衡

內部使用這透過 VPN 來存取應用



情境 3

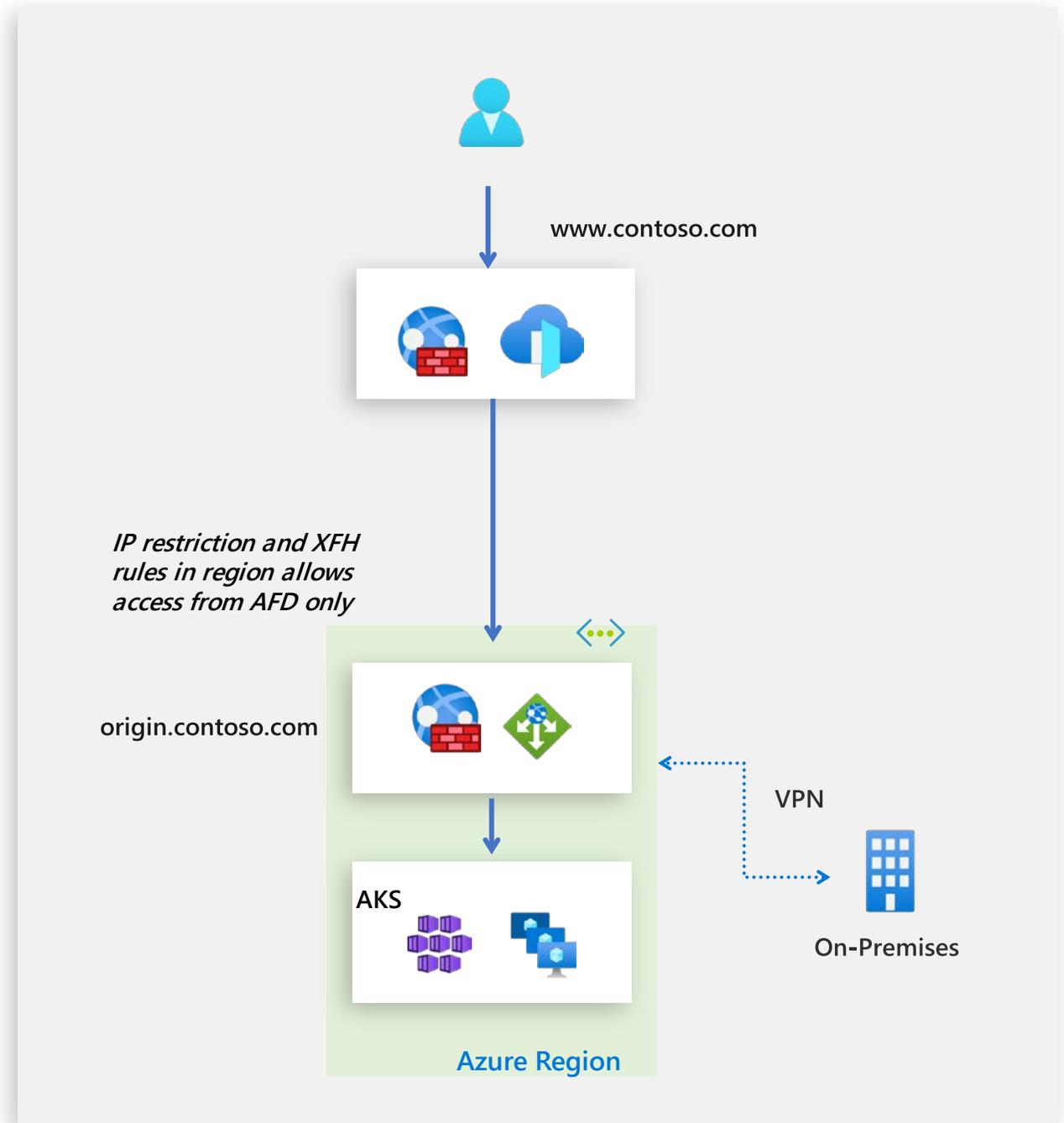
WAF 保護公開以及私人存取的 LOB 應用

WAF 位於網路邊緣 (network edge) 並搭配自訂過濾規則

- ✓ 速率限制
- ✓ 地理限制
- ✓ http 參數過濾

WAF 在 region 中:

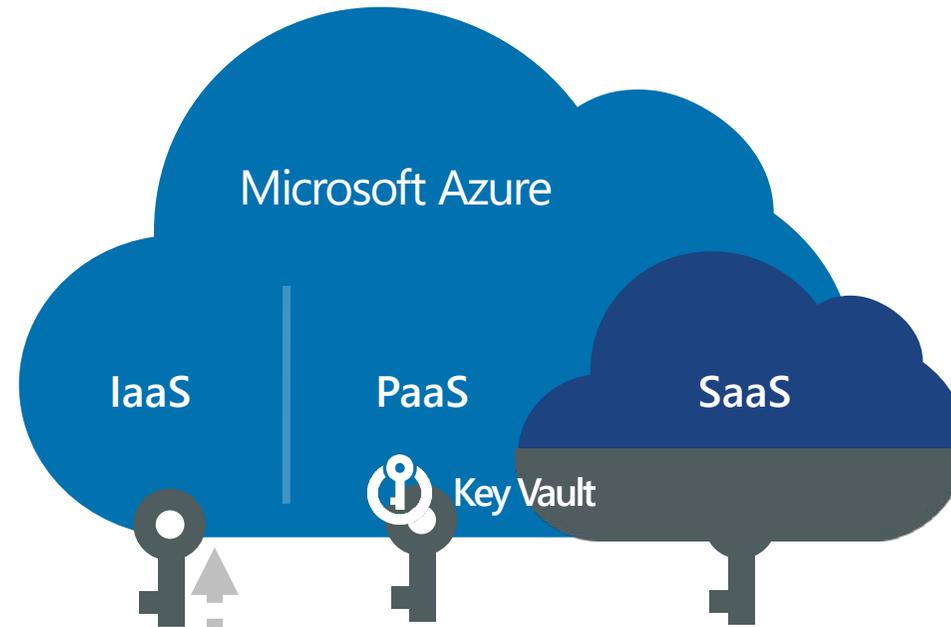
- ✓ 受控規則集
- ✓ 拒絕網際網路直接連線



Microsoft Azure Key Vault

Key Vault 利用 HSMs (硬體加密模組) 提供簡單、高效益的方式來保管您使用在雲端應用的金鑰或秘密

- ✓ 您管理您的金鑰與秘密
- ✓ 應用程式能夠按照您設定的規則條件高效能的取得您的金鑰與秘密

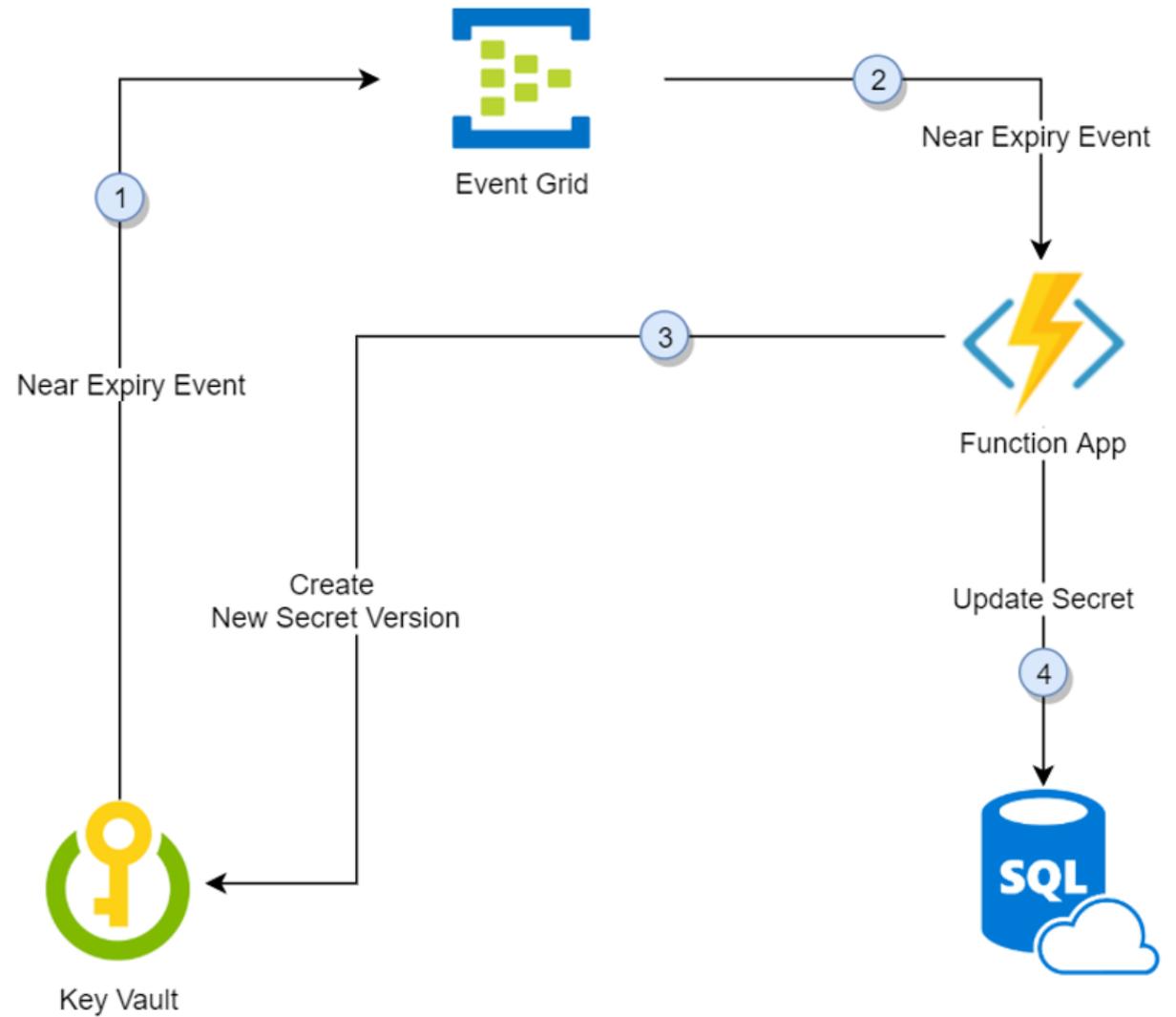


Import
keys

HSM



Azure Key Vault Secret Rotation



保護您的 web 應用程式和 Api

- 啟用適用於 App Service 的 Azure Defender 保護您的 Azure App Service 方案
- 支援方案: 所有App Service方案，及Azure Function方案 (除了Consumption方案)

Home > Security Center

Security Center | Pricing & settings

Showing subscription 'Ju's Microsoft Azure Internal Consumption'

Search (Ctrl+/)

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community

Cloud Security

- Secure Score
- Regulatory compliance
- Azure Defender
- Firewall Manager

Management

- Pricing & settings**
- Security policy
- Security solutions

Pricing & Settings

Configure pricing, data collection and additional settings of your Azure subscriptions and workspaces.

6 MANAGEMENT GROUPS 1 SUBSCRIPTIONS 2 WORKSPACES

Search by name

Name	Azure Defender plan
72f908bf-06f1-41af-91ab-2d7cd011db47 (1 of 2 subscriptions)	
CSS (1 of 1 subscriptions)	
CAPS (1 of 1 subscriptions)	
TPnD (1 of 1 subscriptions)	
Ju's Microsoft Azure Internal Consumption	On (partial)
GSMO-MG (0 of 1 subscriptions)	
ToBeldentifiedMG (0 of 1 subscriptions)	
12LAworkspace	On
judata	On

Home > Security Center >

Settings | Azure Defender plans

Ju's Microsoft Azure Internal Consumption

Search (Ctrl+/) Save

Settings

- Azure Defender plans**
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export
- Cloud connectors

Azure Defender provides enhanced security. [Learn more >](#)

Azure Defender off

- ✓ Continuous assessment and security recommendations
- ✓ Azure Secure Score
- ✗ Just in time VM Access
- ✗ Adaptive application controls and network hardening
- ✗ Regulatory compliance dashboard and reports
- ✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
- ✗ Threat protection for supported PaaS services

Azure Defender on

- ✓ Continuous assessment and security recommendations
- ✓ Azure Secure Score
- ✓ Just in time VM Access
- ✓ Adaptive application controls and network hardening
- ✓ Regulatory compliance dashboard and reports
- ✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
- ✓ Threat protection for supported PaaS services

Azure Defender plan will apply to: 34 resources in this subscription

Select Azure Defender plan by resource type **Enable all**

Azure Defender for	Resource Quantity	Pricing	Plan
Servers	7 servers	\$15/Server/Month	On Off
App Service	2 instances	\$15/Instance/Month	On Off
Azure SQL Databases	2 servers	\$15/Server/Month	On Off
SQL servers on machines	0 servers	\$15/Server/Month \$0.015/Core/Hour	On Off
Open-source relational databases	0 servers	\$15/Server/Month	On Off
Storage	12 storage accounts	\$0.02/10k transactions	On Off
Kubernetes	4 kubernetes cores	\$2/VM core/Month	On Off
Container registries	3 container registries	\$0.29/Image	On Off

Azure Defender 中的 App Service 有哪些優點？

- 使用雲端規模，來識別將 App Service 執行的應用程式視為目標的攻擊。
- Azure Defender在攻擊行為路由到Azure應用程式之前，即會要求經過數個閘道，並在其中進行檢查和記錄。而此資料會用來識別入侵和攻擊者，並了解後續將使用的新模式。
- 您將立即受益於：
 - **安全資訊(Secure)** -產生安全性建議，並依照指示，修正您的 App Service
 - **偵測(Detect)** -Azure Defender 藉由監視來偵測 App Service 資源的許多威脅：
 - 您的 App Service 所在的 VM
 - 對 App Service 傳送和傳送的要求和回應
 - 底層沙箱環境VM
 - App Service Log

Recommendation	Unhealthy resources	Resource health	Initiative	Actions
FTPS should be required in your API App	1 of 1 web applications	ASB	ASB	
Diagnostic logs should be enabled in App Service	16 of 16 web applications	ASB	ASB	
Ensure API app has Client Certificates Incoming client certificates set to On	1 of 1 web applications	ASB	ASB	
PHP should be updated to the latest version for your web app	1 of 1 web applications	ASB	ASB	
FTPS should be required in your web App	16 of 16 web applications	ASB	ASB	
Web apps should request an SSL certificate for all incoming requests	15 of 16 web applications	ASB	ASB	
Managed identity should be used in your web app	10 of 16 web applications	ASB	ASB	
Web Application should only be accessible over HTTPS	7 of 16 web applications	ASB	ASB	
API App should only be accessible over HTTPS	None	ASB	ASB	
CORS should not allow every resource to access your Web Applications	None	ASB	ASB	
Remote debugging should be turned off for Web Applications	None	ASB	ASB	
TLS should be updated to the latest version for your web app	None	ASB	ASB	
TLS should be updated to the latest version for your API app	None	ASB	ASB	
Managed identity should be used in your API app	None	ASB	ASB	
Remote debugging should be turned off for API App	None	ASB	ASB	
Java should be updated to the latest version for your web app	None	ASB	ASB	
CORS should not allow every resource to access your API App	None	ASB	ASB	
Python should be updated to the latest version for your web app	None	ASB	ASB	

Azure Defender 可於 App Service 偵測到哪些威脅？

- 威脅(依 MITRE ATT&CK 策略)
 - **攻擊前的威脅** - Azure Defender 可以偵測到多個攻擊者經常用來探查應用程式是否有弱點的弱點掃描器。
 - **初始存取威脅** - 當已知的惡意 IP 位址連接到您的 Azure App Service 介面時，Microsoft 威脅情報可提供這些警示，包括觸發警示。
 - **執行威脅**： Azure Defender 可以偵測到嘗試使用high privilege來執行指令、於Windows App Service 上欲執行 Linux 指令、無檔案攻擊行為、數位貨幣挖掘工具，以及許多其他可疑且惡意的程式碼執行活動。

Azure Defender 可於 App Service 偵測到哪些威脅？

- 防止無關聯的 DNS 專案，並避免子網域接管風險 (Dangling DNS detection)
- 會在 App Service 網站已解除委任時，識別 DNS 註冊機構中剩餘的任何 DNS 專案
- 風險:遺失子域內容的控制權、從不受信任的訪客搜集 Cookie、網路釣魚行銷活動、其他風險

The screenshot displays the Azure Security Center alert console. At the top, it shows 823 active alerts and 55 affected resources. A bar chart indicates the severity of active alerts: 59 High, 626 Medium, and 138 Low. The main table lists alerts with columns for Severity, Alert title, Affected resource, Activity start time, MITRE ATT&M, and Status. One alert is highlighted with a red box: 'Dangling DNS Record detected on App Service' (High severity, Active status, 01/24/21, 12:41 PM). A detailed view of this alert is shown on the right, including its description: 'A DNS record that points to a recently deleted App Service resource has been detected. This is also known as "dangling DNS" entry and leaves you susceptible to a subdomain takeover. Subdomain takeovers enable malicious actors to redirect traffic intended for an organization's domain to a site performing malicious activity.' The affected resource is identified as 'dangling' (Web application laas) under the 'Playground' Subscription.

Severity	Alert title	Affected resource	Activity start time	MITRE ATT&M	Status
High	Sample alert	Sample-Storage	01/25/21, 11:13 AM	Pre-attack	Active
High	Sample alert	Sample-Storage	01/25/21, 11:13 AM	Exfiltration	Active
High	Dangling DNS Record detected on App Service	dangling	01/24/21, 12:41 PM		Active
High	Azure Security Center...	Openshift-Cluster-1	01/20/21, 01:26 PM	Persistence	Active
High	Azure Security Center...	ASC-Arc-OpenShift...	01/19/21, 07:22 PM	Persistence	Active
High	Azure Security Center...	ASC-Arc-K8S-demo	01/18/21, 01:16 PM	Persistence	Active
High	Azure Security Center...	ASC-Arc-Demo-clust...	01/14/21, 04:50 PM	Persistence	Active
High	Azure Security Center...	aks-engine-arc-test-2	01/14/21, 01:26 PM	Persistence	Active
High	Azure Security Center...	aks-engine-arc-test-2	01/14/21, 01:26 PM	Persistence	Active
High	Azure Security Center...	aks-engine-arc-test-2	01/14/21, 01:26 PM	Persistence	Active
High	Azure Security Center...	microsoft.azuredefe...	01/14/21, 11:12 AM	Persistence	Active
High	Digital currency mini...	app-lx	01/13/21, 12:38 PM	Execution	Active
High	Digital currency mini...	app-lx	01/13/21, 12:38 PM	Execution	Active

保護您的 Key Vault

- 啟用適用於 Key Vault 的 Azure Defender

Home > Security Center

Security Center | Pricing & settings

Showing subscription 'Ju's Microsoft Azure Internal Consumption'

Search (Ctrl+/)

General

Configure pricing, data collection and additional settings of your Azure subscriptions and workspaces.

6 MANAGEMENT GROUPS 1 SUBSCRIPTIONS 2 WORKSPACES

Search by name

Name	Azure Defender plan
72f988bf-86f1-41af-91ab-2d7cd011db47 (1 of 2 subscriptions)	
CSS (1 of 1 subscriptions)	
CAPS (1 of 1 subscriptions)	
TPnD (1 of 1 subscriptions)	
Ju's Microsoft Azure Internal Consumption	On (partial)
GSMO-MG (0 of 1 subscriptions)	
ToBelIdentifiedMG (0 of 1 subscriptions)	
12LAWorkspace	On
judata	On

Navigation menu: Overview, Getting started, Recommendations, Security alerts, Inventory, Workbooks, Community, Cloud Security, Secure Score, Regulatory compliance, Azure Defender, Firewall Manager, Management, Pricing & settings, Security policy, Security solutions.

Settings | Azure Defender plans

Ju's Microsoft Azure Internal Consumption

Search (Ctrl+/) Save

Settings

- Azure Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export
- Cloud connectors

Feature	Azure Defender off	Azure Defender on
Continuous assessment and security recommendations	✓	✓
Azure Secure Score	✓	✓
Just in time VM Access	✗	✓
Adaptive application controls and network hardening	✗	✓
Regulatory compliance dashboard and reports	✗	✓
Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✗	✓
Threat protection for supported PaaS services	✗	✓

Select Azure Defender plan by resource type **Enable all**

Azure Defender for	Resource Quantity	Pricing	Plan
Servers	Loading...	\$15/Server/Month	On Off
App Service	Loading...	\$15/Instance/Month	On Off
Azure SQL Databases	Loading...	\$15/Server/Month	On Off
SQL servers on machines	Loading...	\$15/Server/Month \$0.015/Core/Hour	On Off
Open-source relational databases	Loading...	\$15/Server/Month	On Off
Storage	Loading...	\$0.02/10k transactions	On Off
Kubernetes	Loading...	\$2/VM core/Month	On Off
Container registries	Loading...	\$0.29/Image	On Off
Key Vault	Loading...	\$0.02/10k transactions	On Off
Resource Manager	Loading...	\$4/1M resource management operations	On Off
DNS	Loading...	\$0.7/1M DNS queries	On Off

適用於 Key Vault 的 Azure Defender 警示

- 保護應用程式和認證，即使您熟悉觸發警示的應用程式或使用者，仍務必檢查每個警示的相關情況。
- 警示會出現在 Key Vault 的 [安全性] 頁面、Azure Defender 儀表板和資訊安全中心的警示頁面中

