On Demand Cloud Security for Microsoft Azure

Cloud has gone mainstream and its growth is accelerating as new delivery, management, and security options become available. Important metrics include:

- 94% of organizations are running applications or experimenting with.
- Infrastructure-as-a-Service 87% of organizations are using public cloud.
- Both Amazon and Microsoft generate over $5B annually in cloud services.

Microsoft has invested significantly in the cloud infrastructure, applications, and services to deliver Azure as a highy available global platform. The end result for customers of all sizes—from startups to the largest enterprise—is a trusted cloud platform that enables IT agility in building applications without upfront capex commitment. Microsoft is uniquely positioned in the shift to cloud as they have dominated on-premises applications for decades. Now customers have a choice of on-premises, hybrid, and with a cohesive experience regardless of location.

Current Microsoft customers will benefit from existing licensing and enterprise agreements, making a shift to the cloud easy. In most cases this will lower their overall IT spend—a compelling metric for any CIO/CTO.

Fortinet's cloud security solution is extensible to physical, virtual, and cloud appliances with advanced security orchestration and unified threat protection. It provides more control and visibility by identifying and setting policy by user applications, device specs, IP, and network interfaces. Fortinet delivers the highly optimized solution for Microsoft Azure where application workloads can be protected beyond native Azure security options.

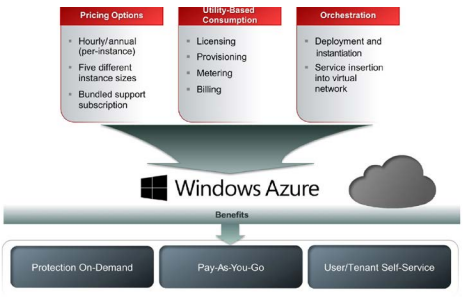
Azure On-Demand Metering

Pay-as-you-go utility consumption allows businesses to make decisions based on workloads. With Fortinet's Azure Resource Manager (ARM) template sizing options ranging from VM02 to VM16, it helps ease scalability and capex concerns.

Bring Your Own License

Fortinet supports a Bring-Your-Own-License (BYOL) perpetual license on Azure with the broadest enterprise security portfolio. Workload-driven security protection, centralized log analytics, and firewall orchestration complement advent use cases running in Azure beyond basic security practices.

The Fortinet cloud security solution can be deployed through the Azure Marketplace with a BYOL model, meaning the license must be procured through a traditional Fortinet channel.



Highlights

- Easy to deploy and manage with best-in-class security capabilities
- Provisions for northbound-southbound access control and east-west traffic auditing in different access security zones
- Complete and consistent Hybrid IT security for Azure Stack
- On-Demand and Bring-Your-Own-License (BYOL) flexible licensing options help cloud-deployment decisions
- Extends workload portability with security vulnerability defense from on-premises to the cloud
- Owns FortiOS, the most powerful security operating system
- Secured by FortiGuard to shield against the latest security vulnerabilities
- Delivers easy Azure Resource Manager (ARM) template for fast configuration and rich API stacks for extended integration

FORTINET Fabric-Ready

One-Stop Hybrid Cloud Security Posture

For many reasons, economics, scale, access, etc., customers might store transactional logs, run one-off campaigns, or branch office workloads on cloud platforms. Fortinet enables you to manage security instance deployments, physical or virtual, to ensure policy consistency across the Fortinet Security Fabric. FortiAnalyzer offers rich and centralized log analytics capabilities to provide the visibility and control in your hybrid cloud deployment.

Whatever the use case, Fortinet makes it easy to manage via a single pane of glass with our full range of available security functions.

Consistent Security Delivery For Hybrid IT

FortiGate NGFW is built for Microsoft Azure Stack with the latest FortiOS update. With the options of virtual domain (VDOM) and non-VDOM FortiGate appliances, Data Center IT can make one vendor security solution for rapid security deployment in the hybrid deployment.

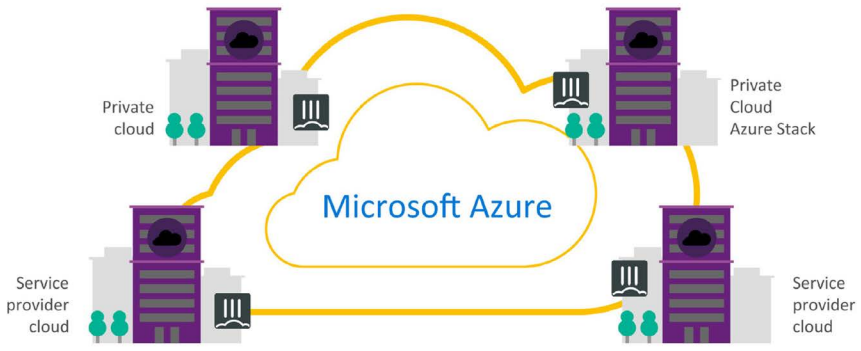
Faster Time to Market and Lower Operating Costs

The Fortinet cloud security products for Microsoft Azure streamline security enforcement with simple templatized virtual appliance deployment options:

- Secure communications between VMs inside a private network
- Secure inbound communications from the Internet
- Secure communications across subscriptions
- Secure communications to on-premises networks

Better Security and Faster Innovation

Many organizations are looking to migrate all systems from on-premises to Microsoft Azure. Fortinet offers the broad set of security portfolio from next-generation firewall, mail security gateway, webt application firewall, centralized policy management to log analytics, etc., in physical, virtualized, and cloud form factors.



The Fortinet Security Fabric is an intelligent framework designed for scalable, interconnected security combined with high awareness, actionable threat intelligence, and open API standards.

Fortinet Security Fabric integration with Microsoft Azure provides the broad, powerful, and automated security protections today's organizations require across their deployments, delivering security without compromise.

Secured by FortiGuard

Knowledge of the threat landscape combined with the ability to respond in real time at multiple levels is the fundamental foundation to providing effective security. FortiGuard Labs delivers global, real-time synergistic protection 24x365 against new and emerging threats. Woven into the full range of Fortinet products, these proactive updates keep your security solution one step ahead.

For more information,
please visit www.fortinet.com/azure
or email azure@fortinet.com

	VM01	VM02	VM04	VM08	VM16
Cores	1	2	4	8	16
Memory (BYOL)	2	4	6	12	24
Instance Sizes	D1v2	D2 D2v2 F2	D3 D3v2 F4	D4 D4v2 A4 F8	D5 D5v2 F16

FORTINET

www.fortinet.com

February 6, 2019 9:14 PM

75602-C-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray