Secure Cloud Migrations with Fortinet and Microsoft Azure

Cloud Migration Strategies

As cloud migrations accelerate, businesses must secure this digital transformation.

All innovation comes with risks and migrating to the cloud is no different. No matter the cloud service provider (CSP), securing data during migration to cloud is important, especially in today’s world where cyber threats grow exponentially and data ecosystems are gaining more complexity. The need to ensure and maintain regulatory compliance and audited records for sensitive data creates even more risk of potential exposure. These threats are not insurmountable, but they do represent a significant risk to a successful migration.

Advanced Security (The Security Fabric)

Securing data effectively in the modern world requires a multipronged approach to cover a wide attack area with a security fabric. This security fabric approach serves to ensure that data is both protected and that all sensitive data meets regulatory compliance and includes each of the following components:

- Zero-Trust Network Access
- AI-Driven Security Operations
- Security-Driven Networking
- Fabric Management Center
- Adaptive Cloud Security

Why Fortinet Next-Generation Firewalls?

Fortinet extends native Azure firewall for advanced protection.

FortiGate Next-Generation Firewall (NGFW) extends beyond Azure’s basic firewall to protect mission critical data and applications with a real, enterprise-class NGFW. This acts as an anchor for the Fortinet Security Fabric. Fortinet also provides powerful central management and is SD-WAN ready. FortiGate enables advanced threat protection, secure connectivity, and automated management for consistent enforcement and visibility across your hybrid cloud infrastructure. SD-WAN Ready.
SOLUTION BRIEF | Secure Cloud Migrations with Fortinet and Microsoft Azure

Fortinet + Microsoft Azure: Unblock and enable secure cloud migration

Fortinet, a global leader in security, offers a single platform for cloud security migration that can help mitigate additional risk by simplifying management and centralizing it into one single platform.

Fortinet Next-Generation Firewalls
NGFWs are network firewalls powered by purpose-built security processing units (SPUs) including the latest NP7 (Network Processor 7). They enable security-driven networking, and are ideal network firewalls for hybrid and hyperscale data centers.

FortiWeb
FortiWeb is a web application firewall (WAF) that protects hosted web applications and API from attacks that target known and unknown exploits. Using machine learning to model each application, FortiWeb defends applications from known vulnerabilities and from zero-day threats.

Fortinet and Azure integration

FortiAnalyzer VM
FortiAnalyzer VM gives critical insights into threats but also accurately scopes risk across the attack surface. This enables organizations to pinpoint where immediate responses are required. It also offers automated responses to threats for near real-time mitigation.

Getting started
Fortinet breaks down the walls that inhibit security visibility and management between and across on-premises and cloud environments. Our security solutions have flexible deployment solutions. Licenses purchased from a Fortinet channel partner for different products are transferrable across platforms. Fortinet solutions, like FortiGate NGFW and FortiWeb WAFaaS can be consumed using a pay-as-you-go (PAYG) on-demand usage model with Microsoft Azure.

Get started with Fortinet solutions on Azure Marketplace:

Fortinet FortiWeb Cloud WAF as a Service

Test Drive - FortiGate NGFW - Single VM with ARM Template

www.fortinet.com