SOLUTION BRIEF

Fortinet Security Fabric Extends Advanced Security for Microsoft Azure

Executive Summary

Microsoft Azure is the cloud of choice for thousands of organizations around the globe. Microsoft Azure supports a variety of security solutions and technologies to protect applications and data in the cloud. But Azure does not provide complete, enterprise-class security. Organizations need deep visibility and granular control security policies—not only within Azure but across other clouds and data centers. This is possible with the Fortinet Security Fabric, which breaks down silos and applies consistent security policies across on-premises and multi-cloud environments and uses threat intelligence from FortiGuard Labs to detect and remediate security events.

68% of enterprise IT departments are using public cloud infrastructure today, and another 27% said that doing so is part of their near-term plan. But cloud security and privacy remain top concerns.[1]

The Cloud Brings New Capabilities and Challenges

Most enterprises either have already undergone or are in the process of evaluating some form of cloud migration. The drivers for this typically include cost reduction and greater business agility. When it comes to securing cloud environments, most cloud providers offer some sort of shared responsibility model for protection. But organizations are still required to establish controls for the hosted applications and sensitive data that they store in the cloud.

To address new vulnerabilities introduced by cloud adoption and other recent digital innovations, many organizations have opted to deploy an array of disaggregated point security products. Upwards of 75 different security solutions are in use at the average enterprise—and many of these only address a single risk exposure or compliance requirement. Beyond the ongoing capital expenses of continuously buying new one-off products, these different solutions typically do not communicate with each other—which increases management burdens while creating new security gaps for threats to slip through defenses.

Securing an Array of Azure Public Cloud Use Cases

As customers adopt Microsoft Azure cloud infrastructures, the need for consistent security across the organization's hybrid-IT infrastructure increases. As part of the integrated Fortinet Security Fabric architecture, Fortinet solutions provide superior visibility, protection, and control for public cloud deployment options in Azure.

1. Secure hybrid cloud

FortiGate next-generation firewalls (NGFWs) and cloud security solutions offer best-of-breed secure connectivity, network segmentation, and application security for hybrid cloud-based deployments. They provide centralized, consistent security policy enforcement using high-speed VPN tunnel connections. FortiGate VMs deployed in the public cloud can securely communicate and share consistent policies with FortiGate NGFWs of any form factor provisioned in a private data center.

2. Cloud infrastructure visibility and control

Fortinet solutions monitor and track all cloud security components—such as configurations, user activity, and traffic flow logs. They also support compliance reporting requirements.

3. Secure access VPN

Remote access virtual private networks (VPNs) enable the use of cloud-based applications. The Fortinet Security Fabric delivers best-in-class performance for securing VPN traffic when remotely accessing Azure. By leveraging Azure's multiregion global infrastructure, organizations can instantaneously scale their services and offer remote access VPN termination close to the end user.

4. Cloud security services hub

Fortinet solutions can be deployed as a transit Azure virtual network (vNET) that allows organizations to share security services to multiple networks worldwide. By leveraging the full extent of Fortinet solutions—including network visibility, VPN connectivity, NGFW, advanced web application firewall (WAF), sandboxing, and mail security—the Fortinet Security Fabric provides far more services while delivering cloud elasticity, on-demand scalability, and optimized price/performance.

5. Container security

Fortinet security solutions are container aware and dynamically integrated into Kubernetes clusters. These are then inserted in the application chain to ensure proper security policies and scanning of container images when deployed.

6. Securing Office 365

Due to the high attachment rate of Office 365 with Azure cloud deployments (alongside the fact that most threats find their way into organizations via email), the need to secure Office 365-based email and business applications is extremely high. The combination of FortiMail, FortiSandbox, and FortiCASB (cloud access security broker) provides critical capabilities when securing Office 365. In particular, the Security Fabric enables deep visibility into mail messages for protection from zero-day threats and monitoring of the Office 365 API layer.

7. Web application security

Web-based applications are vulnerable to a wide range of attacks—both known and unknown. FortiWeb offers a purpose-built WAF that secures APIs as well as front-end web applications to ensure that applications and data remain secure. FortiWeb utilizes machine learning (ML) to self-optimize application protection. FortiSandbox Cloud performs dynamic analysis, including use of artificial intelligence (AI) to identify zero-day threats.

8. Intent-based segmentation

Segmenting cloud environments presents challenges because dynamic provisioning results in constantly changing IP addresses. FortiGate VMs provide intent-based segmentation, which builds rules and segments based on user identity and business logic. Rules are adjusted dynamically in response to a continuous trust assessment. As a result, FortiGate VMs can intuitively define which workloads and elements in the cloud are allowed to communicate with other workloads and elements, whether they are inside or outside the cloud.

How the Security Fabric Complements Azure Security

While Microsoft is responsible for securing Azure's physical cloud infrastructure (e.g., networking and hypervisor), it is up to the customer to ensure that other elements such as communications, access, and applications, among others, are secured and compliant. Customers also are responsible for ensuring that security policies are consistent across clouds and their data centers.

The Fortinet Security Fabric was designed to complement Microsoft Azure security solutions. Fortinet solutions not only run seamlessly in Azure but they also integrate with Azure security services to provide transparency of security policies and events across the cloud infrastructure. Further, Fortinet's native integration with each of the major cloud providers enables seamless, automated, and centralized management across all clouds. This single-pane-of-glass management provides unified visibility, control, and policy management that can scale with additional applications and users. It also reduces the likelihood of security gaps, helps prevent misconfigurations, and ensures that the entire infrastructure is protected by state-of-the-art security.

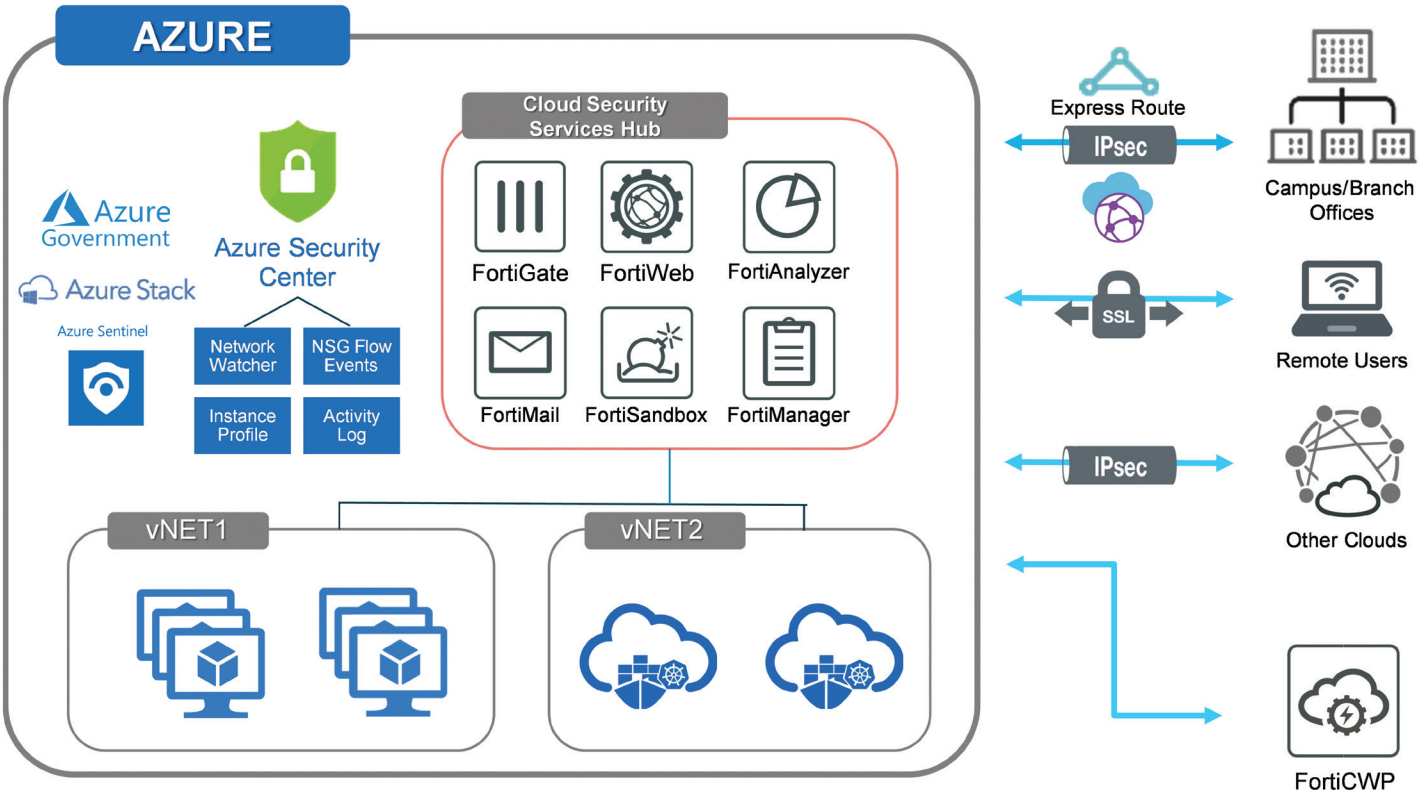

Figure 1: The Fortinet Security Fabric for Microsoft Azure.

Integrated Defenses That Span the Full Attack Spectrum

The different solutions that comprise the Fortinet Security Fabric were designed to increase end-user confidence in cloud environments. The following solutions are part of the Fortinet Security Fabric for Azure:

FortiGate VM NGFW delivers threat protection to defend against the most advanced known and unknown cyberattacks. FortiGate VM scales up and down as business needs change and is offered at various sizes to align with a variety of supported use cases.

FortiWeb WAFs protect web applications from known and unknown exploits. Using ML and AI as well as multilayer and correlated detection methods, FortiWeb defends applications and APIs from known vulnerabilities and zero-day threats. FortiWeb is available as a service as well via pay-as-you-go (PAYG) and bring-your-own-license (BYOL) options.

FortiCWP (cloud workload protection) safeguards workloads and data hosted in Microsoft Azure. FortiCWP hooks into the APIs provided by Microsoft Azure (and other cloud vendors) to monitor and track all security elements—including configurations, user activity, and traffic flow logs. FortiCWP will also scan cloud data stores for sensitive or malicious content and produce compliance reports for common regulatory standards.

FortiMail secure email gateways (SEGs) utilize the latest technologies and threat-intelligence services from FortiGuard Labs to deliver comprehensive protection from common and advanced threats, while integrating robust data-protection capabilities to avoid data loss.

FortiSandbox offers a powerful combination of advanced detection, AI, automated mitigation, actionable insight, and flexible deployment to stop advanced and zero-day threats.

FortiManager provides single-pane-of-glass management and policy controls across the extended enterprise for insight into network-wide, traffic-based threats. It includes features to contain advanced attacks as well as scalability to manage up to 10,000 Fortinet devices.

FortiAnalyzer collects, analyzes, and correlates data from Fortinet products for increased visibility and robust security alert information. When combined with the FortiGuard Indicators of Compromise (IOC) Service, it also provides a prioritized list of compromised hosts to allow for rapid response actions.

Fabric Connectors enable seamless, open integration of Fortinet solutions with third-party security solutions in the Fortinet Security Fabric. This provides automated firewall and network security insertion into dynamic network flows with components in a customer's existing security ecosystem.

Multilayer Protection That Reduces Risk

The Fortinet Security Fabric for Azure helps organizations maintain consistent security protection from on-premises to the cloud within a shared responsibility model. It delivers comprehensive, multilayer security and threat prevention for Azure users. At the same time, it streamlines operations, policy management, and visibility for improved security life-cycle management.

[1] "Enterprise IT Focused on Moving More Workloads to Cloud in 2019," Globe Newswire, January 17, 2019.

November 2, 2019 1:20 PM

535572-0-0-EN

D:\Fortinet\Work\2019\November\110219\sb-advanced-security-microsoft-azure