FORTINET SECURITY FABRIC EXTENDS ADVANCED SECURITY FOR MICROSOFT AZURE

EXECUTIVE SUMMARY

Microsoft Azure is designed to offer a more compliant and secure cloud with easier hybrid cloud migration and coexistence paths. Microsoft Azure supports a variety of security solutions and technologies to protect information in Azure and onsite. Furthermore, Azure offers unique benefits to organizations that have grown accustomed to using Microsoft enterprise services, which are now moving to the cloud via Office 365. But Azure and Office 365 do not provide complete, enterprise-class security features to protect data in the cloud. Organizations need additional deep visibility and granular control over applications and information across the public cloud and on-premises infrastructures. The Fortinet Security Fabric for Azure enables organizations to apply consistent security policies across their multi-cloud infrastructures for enhanced visibility, control, and protection against sophisticated cloud-based attacks.

SECURING AN ARRAY OF AZURE PUBLIC CLOUD USE CASES

The Fortinet Security Fabric for Azure extends consistent, best-in-class enterprise security to Microsoft Azure-based cloud environments. The Security Fabric protects business workloads across on-premises data centers and cloud environments—including multilayer security for cloud-based applications. The Security Fabric supports a variety of common enterprise cloud use cases, including:

1. **Hybrid Cloud.** Businesses need seamless security orchestration that scales along with cloud workloads. The Fortinet Security Fabric includes next-generation firewalls (NGFWs) that complement native Azure security functions while supporting secured and encrypted connectivity across every flavor of cloud infrastructure. They can be managed from either a public cloud deployment or on-premises in a private data center.
2. **Advanced Threat Prevention.** An increasingly essential percentage of modern business applications are deployed over public cloud infrastructures. At the same time, web and mail applications are responsible for the highest number of breaches per pattern. The Fortinet Security Fabric for Azure includes solutions designed to protect these kinds of business-critical applications from known and zero-day attacks by leveraging Security Fabric solutions such as FortiWeb, FortiMail, and FortiSandbox. This helps to relieve the need for constantly applying patches to servers. It also supports compliance with regulatory and security standards such as Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA). Additionally, FortiSandbox can protect collaboration websites from the risks associated with advanced persistent threats resulting from malicious file uploads.
3. **Secure Access VPN.** The Fortinet Security Fabric delivers best-in-class performance for securing VPN traffic for remote access VPN in Azure. By leveraging Azure's multiregion global infrastructure, organizations can instantaneously scale their services globally and offer remote access VPN termination close to the end-user. Remote access VPN can be used to enable access to cloud-based applications as well as on-premises applications that are connected to the cloud over other forms of private links or VPN.
4. **Cloud Services Hub (vNET).** Cloud-provider connectivity far outperforms that of the typical midsize enterprise. An Azure-based virtual network (vNET) allows organizations to share security services to multiple networks worldwide. By leveraging the extent of Fortinet solutions—including network visibility, VPN connectivity, next-generation firewall (NGFW), advanced web application firewall, sandboxing, and mail security—the Security Fabric provides far more services while leveraging cloud elasticity and on-demand scalability for optimized price/performance.
5. **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 as high as ever. The combination of FortiMail, FortiSandbox, and FortiCASB 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.

HOW THE SECURITY FABRIC COMPLEMENTS AZURE SECURITY

The Security Fabric offers deep, multilayer protection and operational benefits for securing applications from known and unknown threats within Azure and for managing global security infrastructures from the cloud. Key capabilities of the Security Fabric for Azure include:

Single-Pane Control and Management. The Security Fabric enables both cloud and on-premises security functionality to be centrally managed from within Azure, which helps eliminate human errors while reducing the time burden on limited IT resources.

Cloud-Native Visibility and Control. Organizations gain in-depth visibility into their Azure application deployments with the Security Fabric. They no longer need to plan for specific deployment configurations, and instead get closer to applying intent-based policy. By using dynamic address groups and logical naming of cloud-based resources, security policies can be extended as Security Fabric resources scale-out across the cloud infrastructure.

Shadow IT Control. With organizations streamlining IT operations and consolidating security controls, many lines of business now directly source their own cloud-based services. The Security Fabric offers IT departments

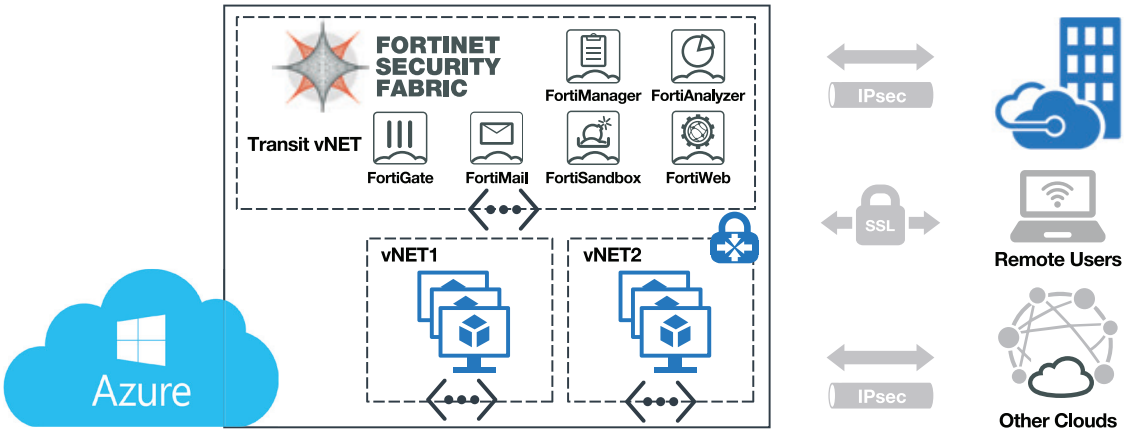

FIGURE 1: THE FORTINET SECURITY FABRIC FOR MICROSOFT AZURE

better visibility into the use of Azure infrastructures and the ability to implement tighter control over usage patterns to protect the organization from risk.

Protection from Zero-Day Attacks. Fortinet Security Fabric solutions offer highly scalable zero-day attack protection that's fully integrated into the cloud infrastructure. This helps to reduce the organization's risk from advanced persistent threats and increases confidence for deploying applications at any scale in the cloud.

Compliance-Ready. Security Fabric solutions offer best-in-class protection to help organizations comply with current industry standards like PCI DSS, as well as the latest data privacy laws such as the EU's General Data Protection Regulation (GDPR).

INTEGRATED DEFENSES THAT SPAN THE FULL ATTACK SPECTRUM

The different solutions that comprise the Fortinet Security Fabric for Azure were designed to increase end-user confidence in Azure cloud environments. All of these solutions are based on Fortinet Virtual Machine (VM) form factors. Licenses purchased from a Fortinet channel partner for VMs are transferrable across platforms. For instance, the same VM license for FortiGate VM on VMware will work for the FortiGate for Azure platform while using the **bring your own license (BYOL)** model. In addition, FortiGate, FortiMail, and FortiWeb can be consumed using the **pay-as-you-go (PAYG) on-demand usage model** directly from the Azure marketplace.

The following solutions are part of the Fortinet Security Fabric for Azure:

- **FortiGate VM NGFW** delivers one of the industry's best threat-protection capability sets to defend against the most advanced known and unknown cyberattacks. FortiGate VM scales up and down with customer requirements and is offered at various sizes to align with a variety of supported use cases.
- **FortiMail** mail security gateways utilize the latest technologies and services from FortiGuard Labs to deliver consistently top-rated protection from common and advanced threats while integrating robust data protection capabilities to avoid data loss.
- **FortiSandbox** offers a powerful combination of advanced detection, automated mitigation, actionable insight, and flexible deployment to stop targeted attacks and subsequent data loss.
- **FortiWeb** web application firewalls (WAFs) protect hosted web applications from attacks that target known and unknown exploits. Using multilayer and correlated detection methods, FortiWeb defends applications from known vulnerabilities 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 (IOCs) Service, it also provides a prioritized list of compromised hosts to allow for rapid action.
- **FortiCASB** provides a cloud-native cloud access security broker (CASB) subscription service that supports visibility, compliance, data security, and threat protection. It offers insights into users, behaviors, and data stored in the cloud via comprehensive reporting tools.
- **Fabric Connectors** enable open integration of the Fortinet Security Fabric to automate firewall and network security insertion into dynamic network flows with multiple existing components within a customer's ecosystem.

MULTILAYER PROTECTION THAT REDUCES RISK

Fortinet breaks down the barriers that inhibit security visibility and management across private, public, and hybrid cloud platforms. It allows security leaders to ensure that their security networks cover the entirety of the attack surface.

The Fortinet Security Fabric for Azure helps organizations maintain consistent security protection in a shared responsibility model, from on-premises to the cloud. 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.

September 23, 2018 6:52 PM

279230-0-0-EN Macintosh HD:Users:ckluck:Documents:FORTINET_ck:Solution-Brief-Microsoft-Azure:Solution-Brief-Azure-2