FORTINET | IBM Cloud

SOLUTION BRIEF

Fortinet Security Fabric for IBM Cloud

Executive Summary

Organizations and agencies rely on IBM Cloud to run their enterprise applications, and those workloads require security that works across clouds and data centers and forms an effective security fabric. This includes consistent security policies as well as deep visibility and granular control wherever compute occurs. By offering single-pane-of-glass firewall management and analytics, Fortinet simplifies security management, reduces security staff workloads, and ensures that applications are protected with the same security policies, whether in the cloud, the data center, or at branch locations.

The Cloud Brings New Capabilities and Challenges

Most enterprises either have already undergone or are evaluating some form of cloud migration, including migrating to IBM Cloud. The drivers for this typically include cost reduction and greater business agility. When it comes to securing cloud environments, IBM does offer a firewall; however, that tool is limited and cannot be used on other clouds or on-premises.

Security without Borders

Applications today may run in a data center, in a private cloud, or in one or more public clouds. A hybrid mesh firewall (HMF) delivers a unified security platform that provides coordinated protection to multiple areas of enterprise IT, including corporate sites such as branches, campuses and data centers, public and private clouds, and remote workers. To do this, HMFs come in various form factors, including chassis, appliances for sites small and large, virtual machines, cloud-native firewalls, and Firewall-as-a-Service (FWaaS), and integrate with other technologies to share security context signals and automation. Fortinet FortiGate VM for IBM Cloud is designed to integrate into your Fortinet Hybrid Mesh Firewall and into your broader Fortinet Security Fabric.

Securing an Array of Cloud Use Cases

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

Secure hybrid clouds

Powered by machine learning (ML) and the latest in artificial intelligence (AI) technologies, 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. FortiGate NGFWs provide centralized, consistent security policy enforcement using high-speed VPN tunnel connections. FortiGate VMs deployed in the cloud can securely communicate and share consistent policies with FortiGate NGFWs of any form factor provisioned in a private data center.

IBM and Fortinet Partnership at a Glance

Valued and trusted partners since 2008, Fortinet works across domains to provide solutions that benefit our broad base of mutual customers. Together, we deliver enterprise-ready cybersecurity solutions that help business leaders protect their digital assets anywhere.

IBM Cloud Solutions

All workloads, from SAP to VMware, can be protected on IBM Cloud and beyond with Fortinet.

IBM Consulting Services

Fortinet is a Global IBM Security Alliance Partner and enables managed services, consulting services, and technology solutions through IBM Consulting that offer comprehensive and unparalleled security protection.

IBM Software

The IBM and Fortinet partnership includes a Fortinet Security Fabric alliance, with an IBM Security QRadar integration that drives other integrations into both SIEM and SOAR in cloud backgrounds.

Cloud infrastructure visibility and control

Fortinet solutions provide a single-pane-of-glass for analyzing security related events across your entire estate. They monitor and track all cloud security components such as configurations, user activity, and traffic flow logs. They also support compliance reporting requirements.

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 IBM Cloud. By leveraging IBM Cloud's multi-region 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 virtual network 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 email security, the Fortinet Security Fabric platform provides far more services while delivering cloud elasticity, on-demand scalability, and optimized price performance.

Zero-trust enforcement

Fortinet solutions, including FortiGate NGFW and FortiWeb WAF, enforce zero-trust policies. Zero-trust network access (ZTNA) solutions grant access on a per-session basis to individual applications only after devices and users have been verified.

Web application security

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

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.

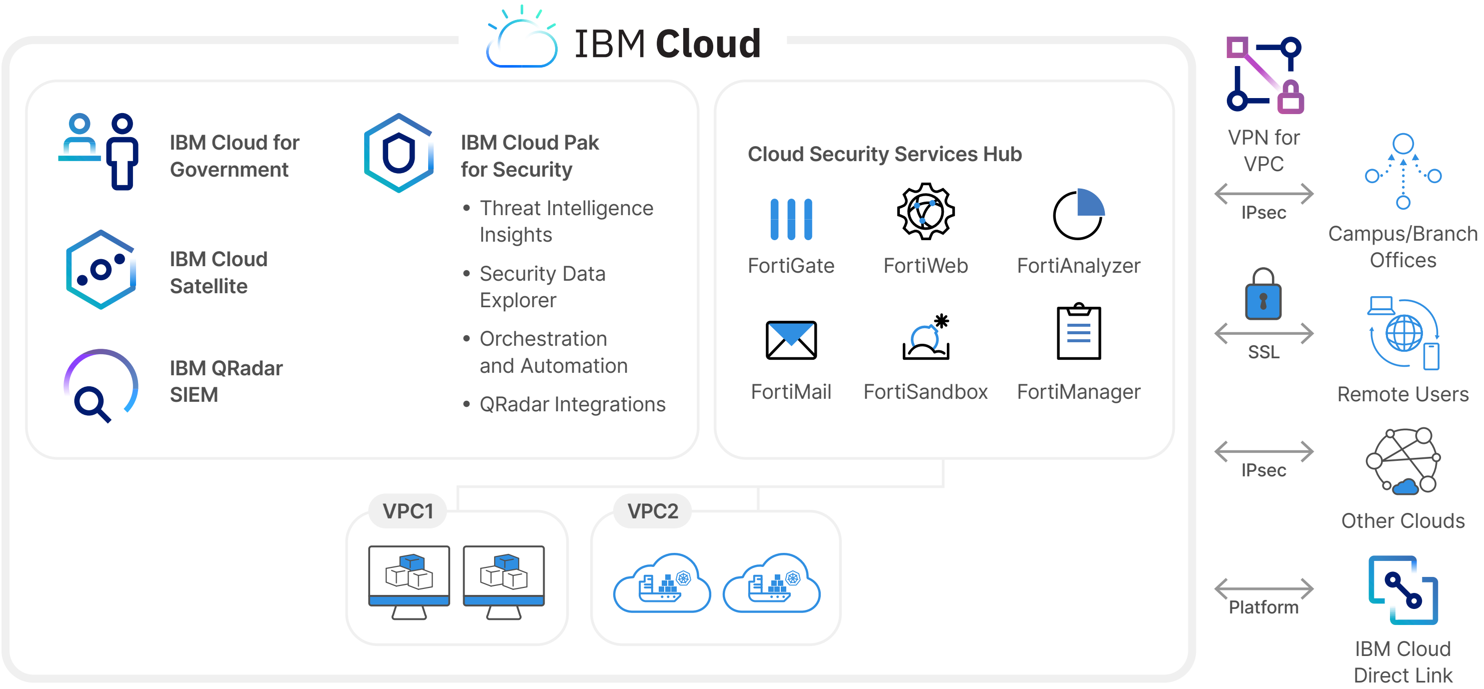

Figure 1: Fortinet secure connectivity for IBM Cloud

How the Security Fabric Complements IBM Cloud Security

While IBM Cloud is responsible for securing its physical cloud infrastructure (such as networking and hypervisor), it is up to the customer to ensure that other elements, such as communications, access, and applications, are secured and compliant. Customers also need to ensure that security policies are consistent across clouds and their data centers.

Fortinet solutions run seamlessly in IBM Cloud and integrate with IBM Cloud security services to provide transparency of security policies and events across the cloud infrastructure. Single-pane-of-glass management provides unified visibility, control, and policy management that scales with new apps and users, reduces security gaps, helps prevent misconfigurations, and ensures the entire infrastructure is protected by state-of-the-art security.

Integrated Defenses That Span the Full Attack Spectrum

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

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 multiple sizes to align with various supported use cases. FortiGate VM is available from the IBM Cloud Catalog.

FortiWeb WAF protects 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.

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 networkwide, 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.

Flexible Consumption Models

Fortinet solutions for IBM Cloud have long been available as PAYG and BYOL licenses. Fortinet's FortiFlex program is a points-based approach that offers organizations the flexibility to scale their security solutions and easily move them from platform to platform. Fortinet solutions for IBM Cloud also help draw down your IBM Cloud Pay-as-you-go with Committed Use.

Multilayer Protection That Reduces Risk

The Fortinet Security Fabric for IBM Cloud 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 IBM Cloud users. At the same time, it streamlines policy management for improved security life-cycle management.

Visit fortinet.com for more information.