FORTINET

STRATEGIES BRIEF

# Key Principles and Strategies for Securing the Enterprise Cloud

## The Fortinet Cloud Security Blueprint

## Executive Summary

**Customers are turning to the cloud to reduce capital expenses and increase agility as part of their digital innovation (DI) initiatives. Despite the benefits, cloud migration results in business-critical data and services being scattered across clouds and data centers. This leads to an expanded attack surface and a corresponding increase in security risk.**

**Some organizations are unknowingly stumbling into a new security paradigm—the shared responsibility model, a model that is built on the assumption that the cloud infrastructure will be secured by cloud providers, while security for services used in the cloud are the responsibility of the organization.**

**The Fortinet Security Fabric was purpose-built to close these cloud-driven security gaps through native integration with public cloud infrastructures, a broad set of security services and products, and cross-cloud security management, automation, and analytics.**

**Enterprises use an average of 61 different cloud applications.[1]**

## Introduction

Fortinet understands that DI is fueling unprecedented growth in cloud adoption. The heterogeneity of the resulting cloud environments expands the overall attack surface. This, in turn, makes it increasingly difficult to protect applications. While public trust in the cloud has increased dramatically over the past decade, security remains one of the top concerns of business and technology leaders. It is critical that security is an integral part of the design process not just for individual cloud solutions but also for the broader, strategic move to dynamic multi-cloud infrastructures.

## A Complex Array of Security Approaches

Cloud providers go to extensive lengths to protect their infrastructure and isolate tenants. Yet, cloud providers vary in their approaches to implementing and managing their native cloud security capabilities. Often, different cloud providers implement the same security functionality, but leverage different tools and approaches.

For example, Amazon Web Services (AWS) extends security policies based on security groups that are associated with cloud resources. The Google Cloud Platform (GCP) uses firewall rules that offer equivalent functionality to AWS but are managed through different interfaces. Many of these differences stem from the unique way that each cloud's underlying architecture is structured and the differing philosophies they have regarding cloud operations.

For customers operating in multiple clouds, the default state of security is a heterogeneous architecture with no central visibility or control, and no consistency in how security is enforced and managed. In this context, each public and private cloud—as well as the on-premises data centers—become independent silos in a fragmented security infrastructure.

## The Cloud Shared Responsibility Model

The shared security responsibility model defines the roles of cloud providers and customers in securing cloud-based applications and data. According to the model, cloud providers are responsible for securing the infrastructure and tenant isolation, while the customer is responsible for securing any resources and services used in the cloud environment. The cloud provider is also responsible for protecting the underlying infrastructure from exploitation, intrusion, and abuse, and must also provide isolation between different customers.

There are different versions of the shared responsibility model based on the type of deployment the customer has. Depending on the type of cloud service offered, the responsibility split between the customer and provider will vary.

In Software-as-a-Service (SaaS) deployments, the customer is limited to a basic set of security controls. For example, it is Microsoft's responsibility to secure Office 365, ensure the application cannot be compromised, and that customers can safely access the application. Customers, on the other hand, are responsible for platform configuration, tracking security events, and data.

Public cloud-based deployments, such as Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS), require the customer to be more deeply involved in security as they lay out larger infrastructures that need to be securely configured and managed. While public cloud providers do offer some security tools, it is incumbent on the customer to select, configure, and manage the security solutions that meet their needs. In this case, the customer is responsible for platform control and configuration, visibility into security events, access control, data encryption, and application security potentially through a web application firewall (WAF). The customer is also responsible for all on-premises portions of hybrid applications.

Customers can turn to a designated security vendor such as Fortinet to provide the broad security they need to protect everything they build, deploy, or store in the cloud.

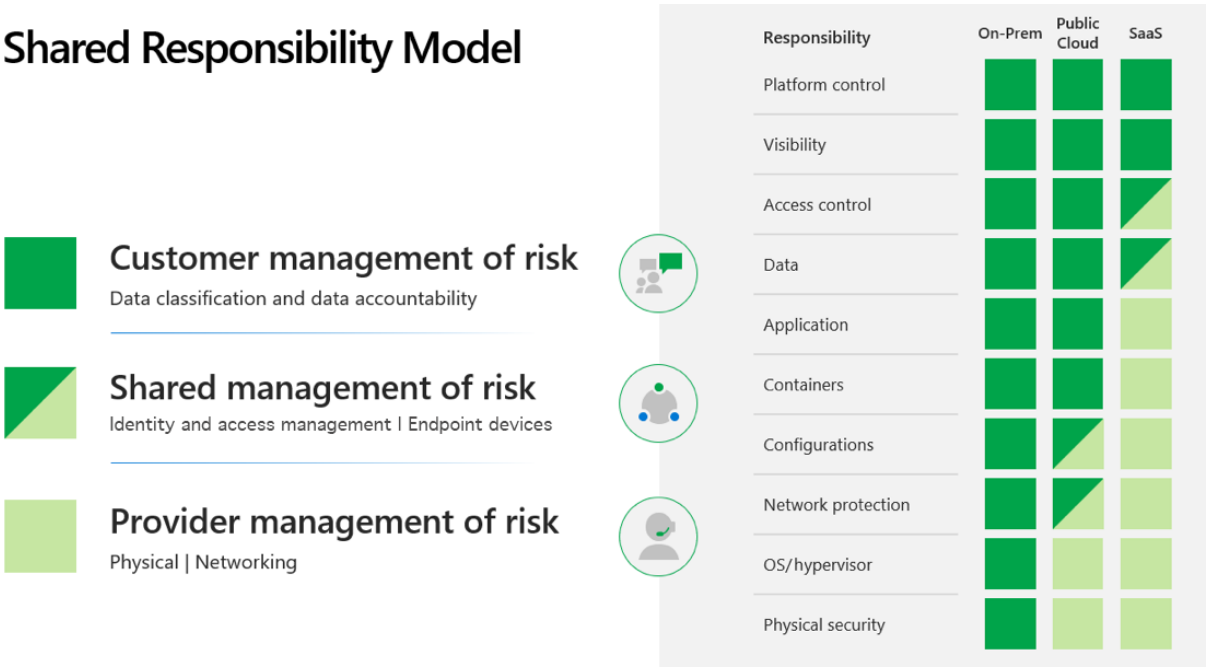


Figure 1: The shared responsibility model shows the customer and the cloud provider are responsible for securing different resources.

## The Elements of Comprehensive Security

Today's evolving threat landscape requires a consistent and unified approach to cloud security. Fortinet follows three overarching principles when designing an effective multi-cloud security solution:

1. Native Integration
2. Broad Protection
3. Management and Automation

An effective cloud security solution must be developed while considering these three elements in order to secure dynamic cloud enterprises. As demonstrated below, Fortinet cloud security solutions have been designed specifically in accordance with these principles.

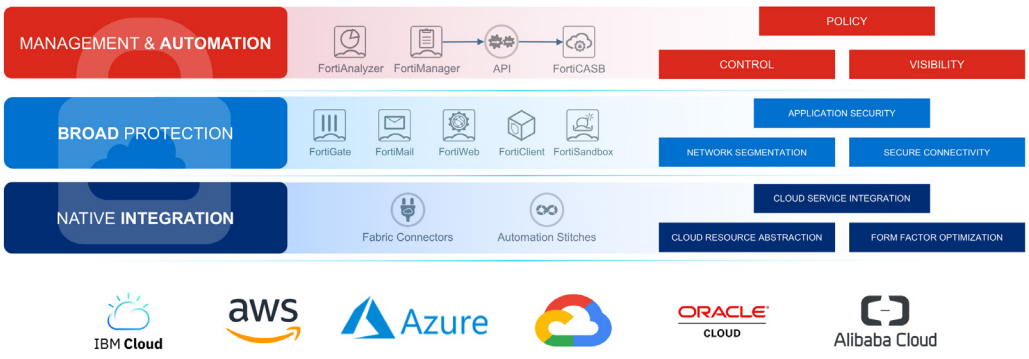


Figure 2: The Fortinet approach to multi-cloud security.

### 1. Native Integration

Fortinet distinguishes itself from other cloud security solution providers through broad, native integration with public cloud platforms. Native integration helps solutions interact with cloud-based information classification as part of the overall security policy management and enforcement capabilities. It is also able to leverage native cloud services for automation, threat monitoring, and tracking. Following are some of the key capabilities of the Fortinet natively integrated cloud security solution:

**Fabric Connectors.** Fortinet security solutions programmatically integrate into the underlying cloud platform to provide maximum security without operational overhead.

Since cloud resources typically use metadata and labels to indicate their logical function or classify information, and IP address information cannot be relied upon to make security decisions, Fabric Connectors can be used to normalize the use of different types of resource metadata across multiple clouds. They help to build and enforce consistent security policies across regions and clouds.

More advanced Fabric Connector implementations learn and list the overall set of cloud resources and represent them in the form of a network topology. This makes it easier for security teams to investigate cloud security posture and to implement effective security policies.

**Optimization.** While some vendors simply port their hardware operating system to a virtual instance, Fortinet solutions are designed from the ground up for cloud deployment. Fortinet solutions fit the needs of a broad set of resource and performance requirements. Solutions range from low-footprint images that maximize the benefits of scale-out architectures, allowing teams to deploy small footprint solutions where needed, to large-footprint solutions that leverage high-capacity networking drivers on different cloud platforms such as Azure Accelerated Networking, Oracle native mode, and AWS C5n instances.

**Automation.** Fortinet makes it easy to automate common tasks, such as responding to different types of threats, by offering automation stitches, automation templates, and robust support for programmatic management via RESTful application programming interfaces (APIs). Automation stitches allow organizations to automate common actions through the GUI without any programming experience or deep cloud domain expertise. Fortinet provides extensive documentation of available APIs for those requiring more flexible and powerful automation capabilities.

**High availability (HA).** Fortinet solutions are designed to be deployed in various HA modes. Each cloud supports HA by leveraging different capabilities. The underlying security must support each cloud environment in a way that offers consistent and predictable security enforcement. In this case, it must support different active/active or active/passive schemes, natively integrating with each cloud to support the availability of business-critical systems.

**Auto scaling.** One of the primary benefits of a cloud infrastructure is its elasticity and on-demand capabilities. This includes the ability to scale services in and out based on varying business needs—paying only for what is used. Fortinet support for native integration with the auto-scaling capabilities of the cloud enables the security infrastructure to keep up with cloud infrastructure scaling based on volume and demand, ensuring that applications are continuously protected.

**Configuration templates.** Templates can both reduce errors and help automate key processes such as auto-scaling cloud deployments. Fortinet configuration templates support a variety of frameworks, such as AWS CloudFormation Templates (CFT), Azure Resource Manager (ARM), HashiCorp Terraform, and Ansible, to help security administrators provision solutions quickly and accurately across various cloud platforms and to meet the needs of cloud workload deployments. Configuration templates help to reduce the potential for human error while accelerating the ability to attach security to new workloads and, in turn, ensuring that security administrators confidently deploy new workloads.

**Service integration.** Cloud platforms offer software and platform services that simplify the consumption of various capabilities by eliminating the need for users to master each technology. It is critical that security solutions integrate with each cloud platform and offer security functionality as part of the native service consumption model. Here, integration extends security protection to more use cases and services as a fundamental capability, offering basic protection for experimentation environments as well as those that are not yet part of a broader security management life-cycle routine.

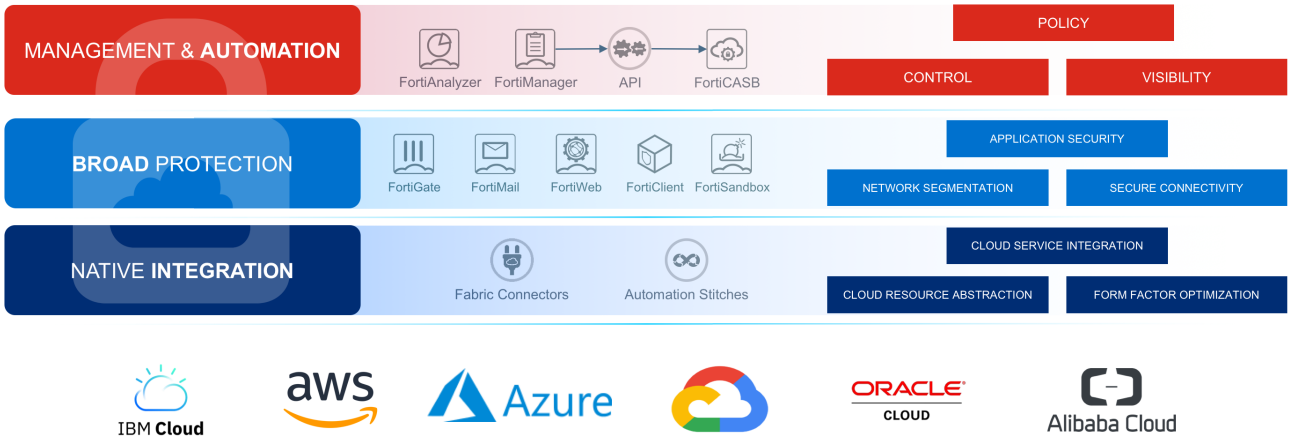


Figure 3: Three pillars of multi-cloud security.

### 2. Broad Protection

Fortinet offers the broadest and most complete security portfolio in the industry, providing enterprise-class network and application security, as well as secure access products that share intelligence and work together to form a cooperative fabric. The Fortinet Security Fabric combines an intuitive operating system, multiple layers of threat detection, and applied threat intelligence to deliver security, visibility, and control.

Security teams can reduce and manage the attack surface through integrated visibility, prevent threats through integrated artificial intelligence (AI)-driven breach prevention, and reduce complexity through automated operations and orchestration. Learn more about how Fortinet delivers broad protection for the cloud:

**Zero-day threat protection.** New zero-day, previously unknown threats are found nearly every day, and impact both cloud and on-premises deployments. As attackers increasingly employ AI and machine learning (ML) technology, the number of zero-day threats is likely to grow.

Fortinet provides a number of technologies for identifying and stopping zero-day threats, including sandbox analysis that observes potential malware in a simulated environment. The sandbox then determines if it can execute safely and be examined with behavioral tools for malicious intent.

However, sandbox analysis is time- and processor-intensive, and can slow performance to a crawl if most traffic is not prefiltered. Fortinet employs AI and ML for threat detection through analysis of characteristics, catching many threats before they need to be subjected to sandboxing. The ability to deploy sandboxing technologies, either in an IaaS-VM or as a SaaS application, is a critical capability that should be part of any multi-cloud security strategy.

**SSL and IPsec VPN.** Extending secure connectivity into and across clouds is critical. As traffic flows across the internet and cloud environments, the ability to isolate traffic and build consistent networking security policies are key enablers to unifying disparate cloud environments. The support of both site-to-site IP security (IPsec) VPNs and VPNs across virtual cloud networks is essential to consistently secure and isolate traffic. VPN implementations should be interoperable with different cloud VPN solutions, offering flexibility for different organizations and organizational units. Furthermore, the ability to deliver high-speed VPN connectivity is key. FortiGate VM is optimized to deliver secure, high-throughput connectivity without slowing cloud-based applications.

**Application control.** Application control from FortiGuard services enforces security for internet-based applications and enables organizations to quickly create policies to allow, deny, or restrict access to applications. This service offers visibility and control of thousands of applications and allows organizations to add custom applications. Teams can fine-tune security policies based on application type and optimize bandwidth with application-driven traffic management.

**Secure SD-WAN.** Fortinet has redefined the SD-WAN market by including its best-of-breed next-generation firewall (NGFW), SD-WAN, advanced routing, and WAN optimization capabilities, delivering a security-driven networking WAN edge transformation in the unified FortiGate offering. A secure cloud connection is also critical to support seamless security operations. Fortinet received an NSS Labs “Recommended” rating in the SD-WAN group test and delivered the lowest total cost of ownership (TCO) per Mbps among all eight vendors.[2]

**Zero trust.** Networks designed with implicit trust simplify the ability for data and applications to move around inside the perimeter. This contributes to network breaches that can remain undetected, allowing malicious insiders to steal critical data. The FortiGate VM NGFW supports dynamic segmentation that utilizes logical attributes of data and applications across multiple locations and the cloud to provide consistent isolation of resources with zero assumptions, validating every connection regardless of VLAN or origin network.

**NGFW.** With organizations building more business-critical applications in the cloud, there is a greater need for advanced security capabilities. FortiGate virtual appliances for both ingress and egress security offer the same breadth of security functionality for the cloud as they do on-premises. Additionally, these solutions deeply integrate with various cloud platforms and are optimized to deliver high performance in cloud infrastructures.

**Web application firewall (WAF).** As DI fuels transition to business-critical applications, new applications are increasingly web-based. The FortiWeb WAF delivers threat protection for critical web applications and APIs. FortiWeb offers ML-based threat prevention and bot mitigation capabilities that fine-tune web security policies and eliminate false positives. FortiWeb helps organizations address the requirements of risk management policies and regulatory requirements related to protecting end-user information and ensures business continuity.

**Email security.** Email remains a common vector for malware, particularly as organizations migrate email systems to the cloud and rely on them as backup systems. By the end of 2022, cloud business email accounts are expected to account for 87% of all business email accounts.[3] Fortinet email security solutions deliver complete protection from email-borne threats in the cloud and on-premises, and are ideally suited to support cloud migration.

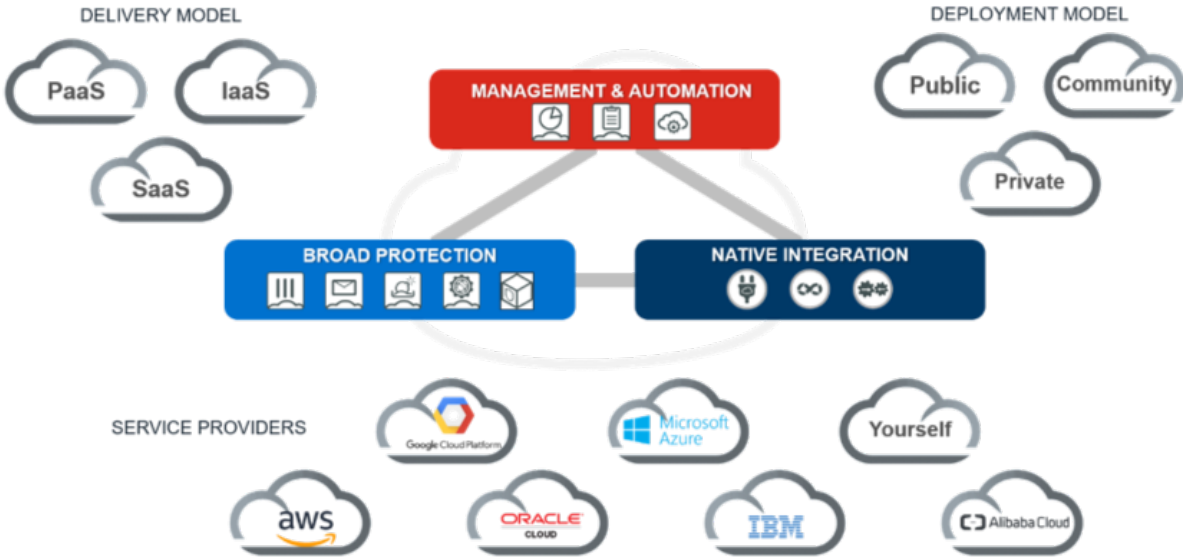


Figure 4: A comprehensive solution that works across different delivery models, deployment models, and service providers.

### 3. Management and Automation

Unifying an organization's security infrastructure not only eases management but also helps ensure that consistent security policies are applied wherever applications run, data is stored, or infrastructure is built. In addition, it enables the automation of security life-cycle management processes and helps ensure compliance. These capabilities allow organizations to manage cloud and on-premises infrastructures similarly by leveraging the same level of visibility and control. Centralized management and automation help organizations meet risk management and regulatory compliance objectives.

Effective security management and automation consists of four primary elements: visibility, control, policy, and compliance. Fortinet enables these elements with its suite of management products including FortiManager, FortiAnalyzer, FortiCASB, and FortiCWP cloud workload protection (CWP).

**Visibility.** The ability to consistently see all applications, networks, infrastructures, security events, and logs in a multi-cloud environment is a cornerstone of a security posture assessment. Such assessments are both a starting point and an ongoing process of security management. Organizations need to identify resources spread throughout the infrastructure, associate traffic flows, understand which

applications are being used, and identify what data traverses the network. FortiAnalyzer provides inline visibility across Fortinet systems for deep analysis, and FortiCWP provides visibility into the entire public cloud stack, leveraging cloud-specific APIs.

This information allows an organization to validate whether security policies are effective, and if additional security policies are needed. In a multi-cloud environment where applications communicate across the various infrastructures, the ability to centrally trace traffic flows and understand the sequence of events across each cloud environment often offers more insight than what standard security tools reveal. In addition, the ability to tie security infrastructure insights with cloud infrastructure visibility into a single pane of glass further simplifies operations.

**Control.** Once an organization has full security visibility, the next step is to apply controls to relevant functions. This involves applying configuration changes and populating the security infrastructure with the relevant resource-related information pertaining to the multi-cloud security posture. Security management tools should extend a consistent control framework across the broad set of security functions.

Additionally, the control framework should extend to the native security functionality provided by each cloud platform. This allows administrators and operators to apply security changes throughout the infrastructure, regardless of the underlying technology. FortiManager helps administrators apply consistent policies across infrastructures.

**Policy.** Leveraging the visibility and control capabilities of the Fortinet Security Fabric enables organizations to gain consistent security management and enforcement throughout the infrastructure. Since the overall application life cycle is what drives changes to the infrastructure, the burden and time to interpret how changes to applications affect the infrastructure are significantly reduced. Instead, security staff can modify security settings in accordance with application life-cycle events to achieve more consistent security policies.

FortiCWP helps identify policy misconfiguration and compliance violations. It uses threat intelligence and native integration to assess configurations, monitor activity in cloud accounts, monitor cloud network traffic, analyze and scan data, and provide compliance reports.

FortiManager further aids in multi-cloud policy management by enabling organizations to manage all of their Fortinet devices from a single console. It provides full visibility of the network, offering streamlined provisioning and automation tools.

Security staff can leverage these capabilities to shift to a strategic security posture by rapidly implementing policies in a centralized platform that allows for faster updates.

**Compliance.** Maintaining a consistent security posture and automating security operations significantly increases an organization's ability to maintain regulatory compliance. In addition, centralized security management, automated workflows, and shared threat intelligence help organizations quickly react to emerging threats. They also can more effectively mitigate risk across their entire attack surface without requiring overly challenging security operations. FortiCWP and FortiCASB meet the compliance needs of organizations by identifying compliance issues and providing reports on compliance status.

**Security and Threat Research**

This blueprint documents the primary elements of implementing effective solutions for consistent hybrid-cloud security with native integration, broad protection, and management and automation. However, technology alone is not sufficient. A world-class cloud security solution must include security intelligence-based services that are used as data sources for the products determining threats. These services should be backed by security experts with the skills and resources to master the rapidly changing world of cybersecurity.

FortiGuard Labs boasts one of the largest security research and analyst teams in the industry with experts around the world. These dedicated experts are always on the lookout for breaking threats and new techniques—studying every critical area of the threat landscape including malware, botnets, mobile, and zero-day vulnerabilities.

Additionally, FortiGuard Labs maintains an integrated threat-intelligence ecosystem with more than 200 security intelligence partnerships and collaborations. The combination of an industry-leading research and analyst team with an extensive security intelligence ecosystem allows Fortinet to provide the leading-edge detection and protection organizations need to prevent, detect, and address new threats from the onset.

## Cloud Security Use Cases

There are a variety of cloud adoption initiatives and security use cases to consider when approaching a cloud security strategy. The appropriate use cases for different cloud initiatives can vary. Often organizations engage in one of three types of cloud adoption initiatives as follows:

- Consuming SaaS applications
- Building cloud-native applications
- Migrating or extending existing applications to the cloud

All three initiatives require different security solutions to maintain a strong security posture and operational model. While the shared responsibility model provides useful guidance, most organizations will need to extend their visibility and control throughout the cloud regardless of the type of cloud adoption initiative they are taking on.

While the overarching goal of increasing cloud visibility, control, and protecting applications is paramount with all three initiatives, the use cases and specific products to meet each goal will differ. The three solution families for cloud security offered by Fortinet are: (1) visibility and control, (2) application security, and (3) secure connectivity. The following section explains the different use cases associated with each solution.

### Fortinet Cloud Security Use Cases

**1. Visibility and Control**

- SaaS visibility and control
- Cloud infrastructure visibility and control
- Compliance in the cloud
- Cloud-based security management and analytics

**2. Application Security**

- Web application security
- Logical (intent-based) segmentation
- Container security
- Secure productivity
- Cloud workload protection

**3. Secure Connectivity**

- Secure hybrid cloud
- Cloud security services hub
- Secure remote access

## 1. Visibility and Control

### SaaS Visibility and Control

IT teams and line-of-business leaders alike have embraced SaaS as a flexible, scalable, cost-effective way to deploy business-critical applications. The issue is that as the use of SaaS grows, usage is often unregulated, and security is often treated as an afterthought. Effective cloud security must monitor all SaaS activity and integrate with security solutions to enforce uniform security policies across both traditional and SaaS-based applications.

Fortinet delivers centralized control of SaaS applications so organizations can deploy best practices with regard to compliance and governance. It also helps organizations protect sensitive data in applications from advanced threats and brings Shadow IT applications under centralized control. Organizations also gain consistent application-control policies across all of a company's branch locations. Enhanced security also helps reduce latency and provides the level of performance that users expect.

FortiCASB provides centralized, detailed visibility on all SaaS application usage. This enables organizations to implement uniform application-control and security policies, protect their sensitive data against advanced threats, and support security compliance and governance.

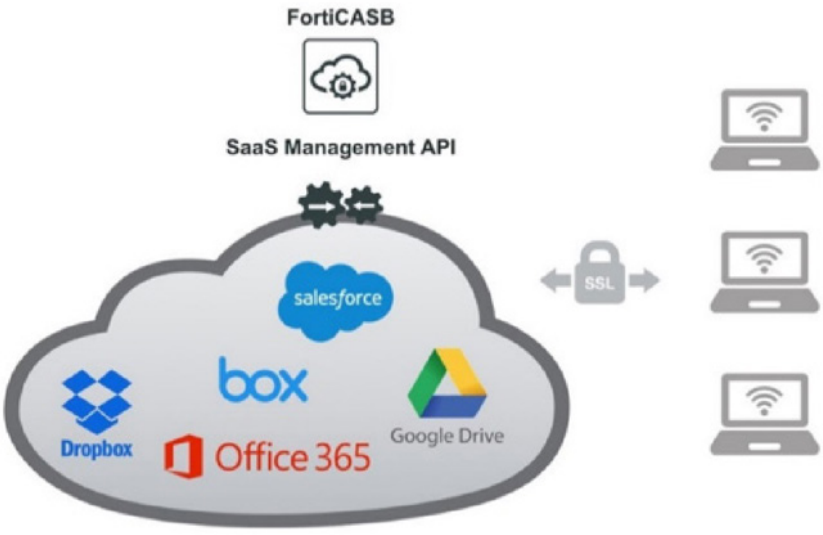


Figure 5: Public cloud security use cases.

### Cloud Infrastructure Visibility and Control

As cloud use increases, so does the likelihood of misconfiguration. In addition, since public cloud usage is not always monitored, it can lead to unchecked vulnerabilities.

FortiCWP leverages the public cloud management APIs to monitor activity and configuration of multiple cloud resources. It continuously evaluates configurations across regions and public cloud types and provides consistent visibility. FortiCWP simplifies compliance violation reporting and enhances compliance by providing guidance on security best practices. It also offers threat and risk management tools that help trace misconfigurations to their source. FortiCWP supports AWS, Google Cloud Infrastructure, and Microsoft Azure.

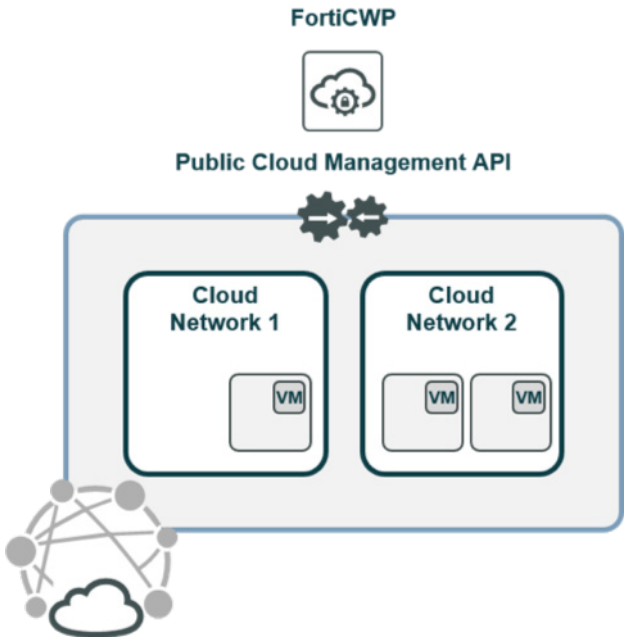


Figure 6: FortiCWP uses public cloud-native APIs to monitor security activity and configuration across clouds.

### Compliance in the Cloud

Achieving compliance with PCI DSS, HIPAA, SOX, GDPR, and other regulatory mandates can be a time-consuming burden. Migration to the cloud or multiple clouds only increases this burden. Fortinet cloud compliance solutions include:

**FortiCWP**, which aggregates and organizes security information from multiple cloud services and APIs into meaningful compliance reports and live compliance dashboards.

**FortiSIEM**, which provides a broader view of compliance across multiple clouds, the Fortinet Security Fabric, and third-party products. It can create compliance reports at the push of a button.

**FortiAnalyzer**, which collects logs from Fortinet Security Fabric elements, and FortiManager enables changes to be audited, reviewed, approved, and implemented. Together, they close the loop on compliance gap mitigation. All systems support automated processes to facilitate compliance policy management

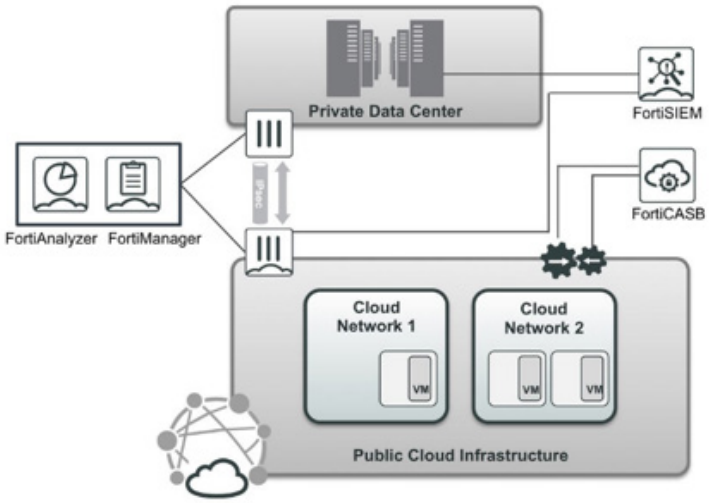


Figure 7: Fortinet solutions for cloud compliance.

and workflow, reducing risk when policies are changed.

### Cloud-based Security Management and Analytics

Using legacy management tools alongside new technologies creates complex incompatibilities, especially when seeking to manage from the cloud.

To solve these challenges, organizations can leverage the multi-regional and global presence of top cloud infrastructure providers to deploy centralized and global security management and analytics systems in the cloud. FortiManager VM, FortiAnalyzer VM, and FortiSIEM VM can all be deployed in the cloud to scale and globalize. Benefits include:

- Centralized, unified security management and visibility
- Enhanced audit and compliance reporting
- Faster incident response

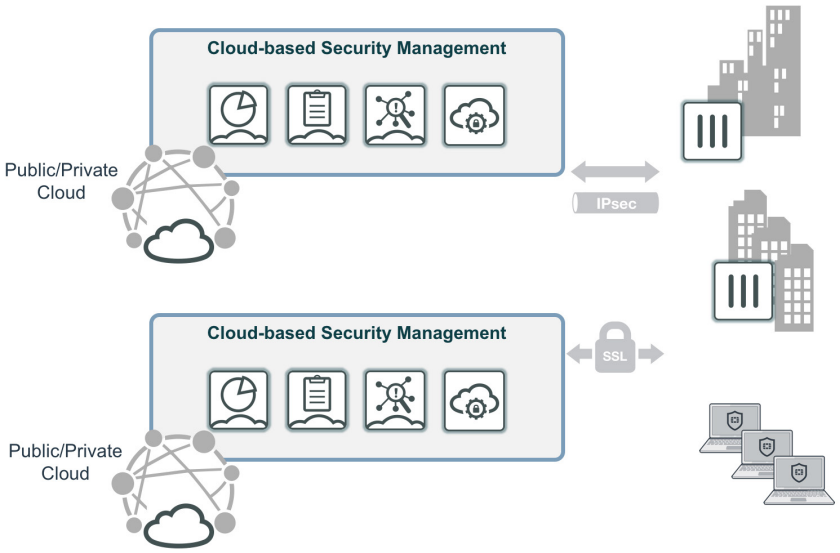


Figure 8: Fortinet solutions for cloud-based security management and analytics.

- Improved operational and cost efficiency, reducing risk
- Increased ability to automate security management

## 2. Application Security

### Web Application Security

Cloud-based applications often use web services to communicate internally as well as outwards, leaving applications vulnerable to various threats. Additionally, the organizations operating these applications are often burdened with meeting compliance requirements.

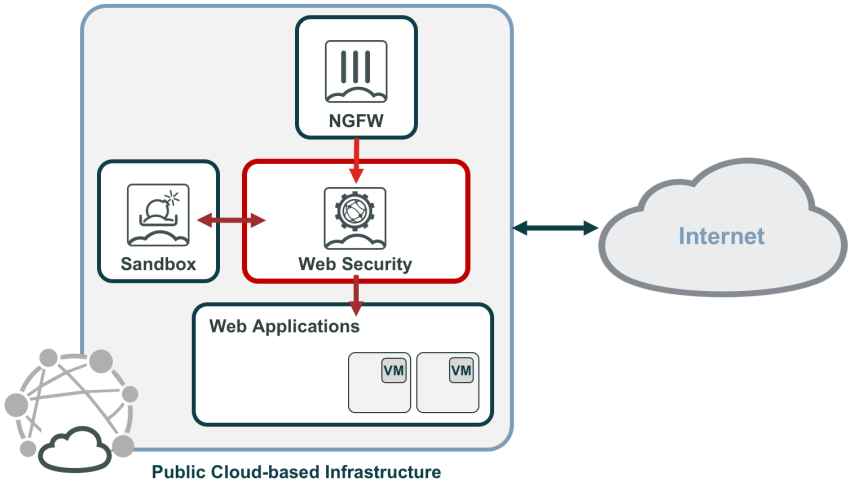


Figure 9: Fortinet protects applications against known and unknown threats.

Fortinet offers a variety of web application security solutions that are ideally suited for cloud-based customers. FortiWeb VM, an industry-leading WAF offered on all major cloud platforms, secures web services APIs as well as front-end web applications from known and unknown threats. Through integration with FortiWeb, FortiGate VMs centrally enforce security policies and provide increased visibility. The Fortinet sandbox service performs dynamic analysis to identify previously unknown malware.

### Logical (Intent-based) Segmentation

Segmenting cloud environments is challenging because dynamic provisioning results in constantly changing IP addresses. Network segmentation based on static IP address rules is therefore ineffective.

FortiGate VMs provide intent-based segmentation, which builds access rules and segments based on user identity or business logic and adjusts rules dynamically in response to a continuous trust assessment. FortiGate VMs leverage metadata or tags associated with cloud-based resources across multiple clouds to enforce security policies. As a result, they intuitively define which workloads and elements in the cloud are allowed to communicate with other workloads and elements, and whether they are inside or outside the cloud.

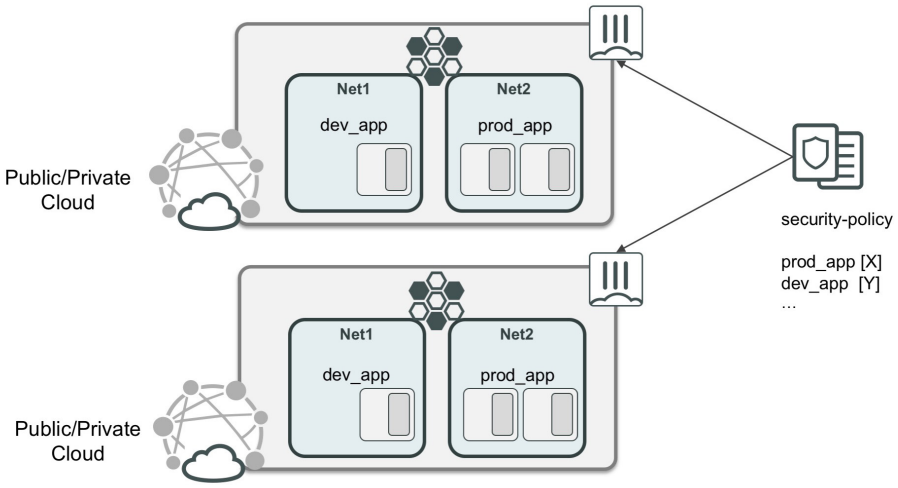


Figure 10: Logical segmentation.

### Container Security

Containers have rapidly become a key element in cloud computing. Containers are popular because they allow applications and their dependencies to be packaged so the application can be reliably moved from one computing environment to another. Containers isolate software from the operating system and underlying hardware, ensuring the application will work wherever it resides.

Container security starts with the protection of the integrity of the underlying containers. It also takes a step further, securing the container pipeline, the infrastructure the container runs on, and the commands and data planes supporting the containers.

The Fortinet container security solution is divided into four complementary areas of protection. Container-aware security with the Fabric Connector enables awareness of container labels when defining security policies. FortiGate can play a critical role in securing north-south traffic into and out of containers. FortiGate NGFWs offer Fabric Connectors that interface with major container orchestration systems to leverage metadata as security policy objects, including native Kubernetes, AWS EKS, GCP GKE, Azure AKS, and OCI OKE.

**FortiWeb** as a container image can be bundled within an application chain. Container-integrated security allows a Fortinet solution to be dynamically integrated into Kubernetes clusters and inserted in the application chain, providing web application security to container-based apps.

**FortiSandbox** provides container registry security by scanning pulled, preconfigured container images for malicious code and zero-day threats. Finally, FortiNAC can ensure that the application and its container can be accessed only by those in the appropriate roles with the appropriate privileges.

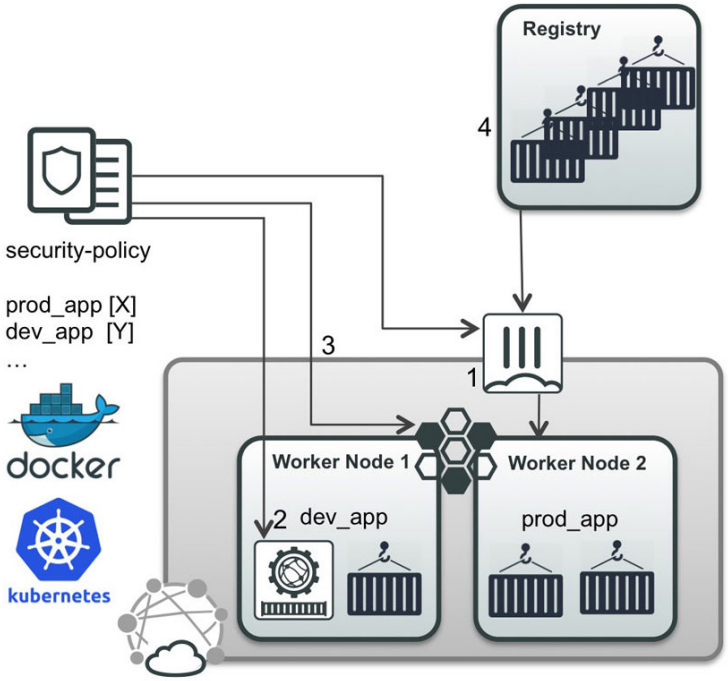


Figure 11: Container security.

### Secure Productivity

As organizations increasingly outsource the IT management aspect of productivity and email applications, the visibility and control over these applications is reduced. Security teams need the ability to provide consistent purpose-built security across multi-cloud environments.

The combination of FortiMail, FortiSandbox, and FortiCASB-SaaS provides critical capabilities when securing business productivity applications such as Microsoft Office 365. The Security Fabric enables deep visibility into application traffic, and Fortinet security services and sandbox technology identify and block zero-day and advanced persistent threats.

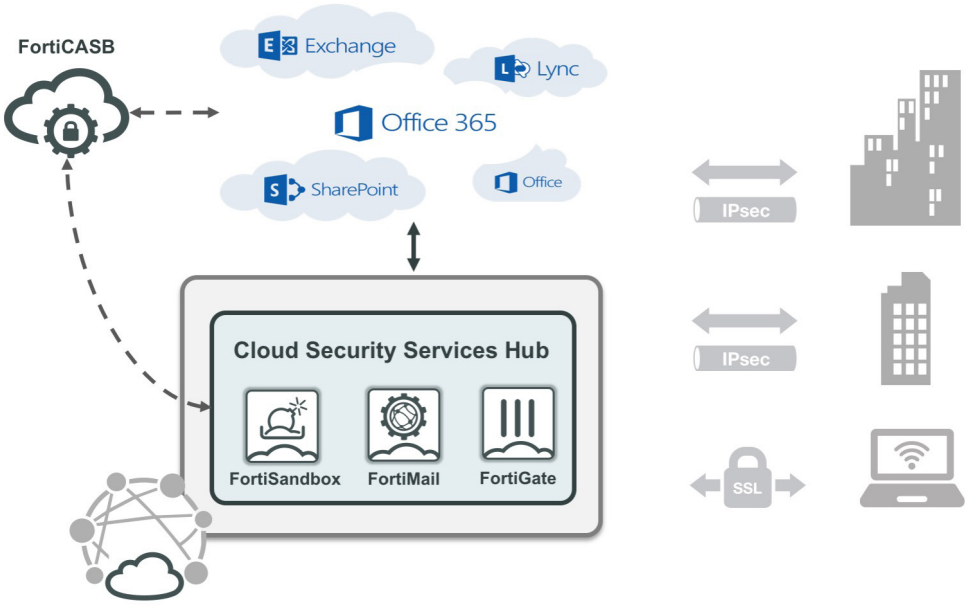


Figure 12: Fortinet secure productivity for cloud.

### Cloud Workload Protection

Applications built in or migrated to the cloud need to be protected against traditional internet-originated threats, as well as from new threats that propagate across workloads and are introduced via APIs.

The combination of inline protection for north-south traffic, host-based protection for east-west traffic, and protection for cloud API and configuration risks offers the tightest security solution for the cloud. Leverage FortiGate VM to protect your virtual cloud networks from internet-originated threats as well as providing inter-cloud secure connectivity. Extend security within the cloud by using FortiClient on VMs, assuring compliance and connectivity. FortiCASB-Cloud protects from unwanted or unsupervised configurations at the cloud-account level.

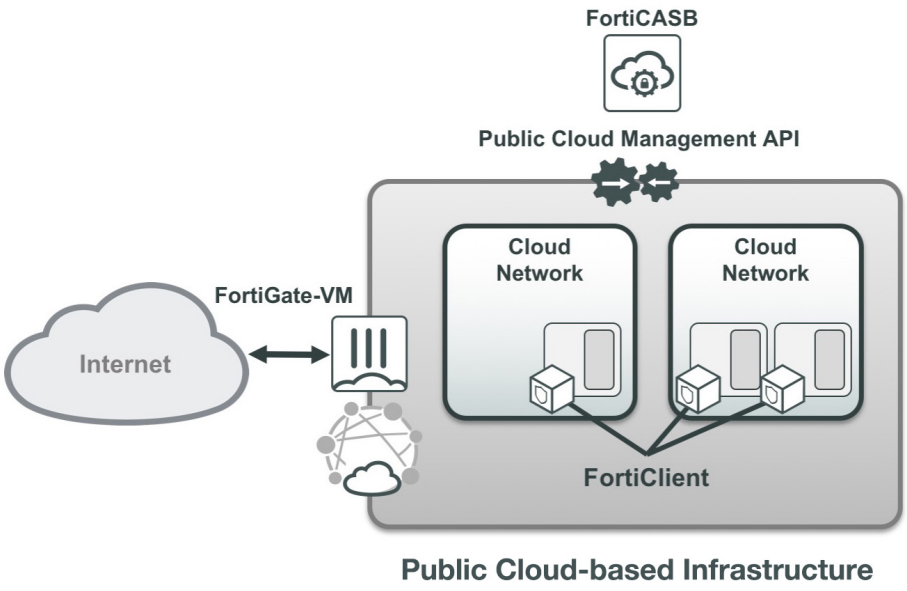


Figure 13: Fortinet cloud workload protection.

## 3. Secure Connectivity

### Secure Hybrid Cloud

Many organizations leverage the public cloud to provide infrastructure for IT solutions alongside on-premises data centers. In many cases, new applications are uniformly deployed to the public cloud, while in other instances they are deployed across public and private clouds in parallel.

It is important for a solution to offer support for both private cloud and public cloud technologies. It must also deliver fast and powerful security in order to cope with high-volume data transfers. Consistent management of security policies is critical, too. This ensures migration of applications from one infrastructure to another does not incur unwanted security operational overhead that could potentially result in human error that compromises security. Additionally, security must protect the entire attack surface and scale to accommodate constant change.

FortiGate NGFW 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 and connect through a high-speed VPN tunnel. 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.

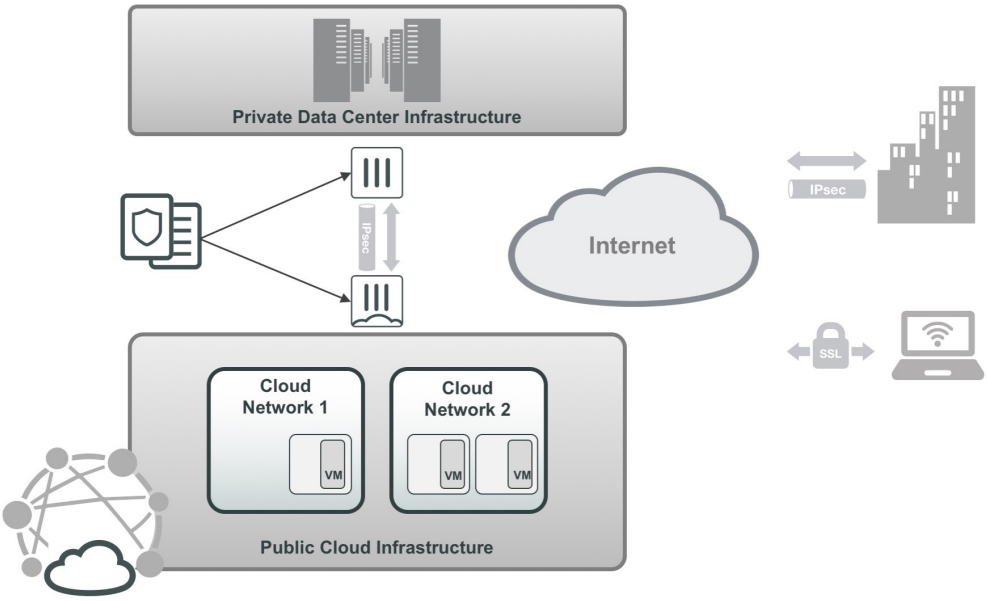


Figure 14: Secure hybrid cloud.

### Cloud Security Services Hub

When teams develop applications in separate virtual networks and clouds, there is no centralized security management, making it challenging to secure the resulting applications and separate environments.

Security teams looking to unify disparate environments need a centralized security services hub, or transit network. The hub splits security from application development to provide centralized, shared, and consistent security enforcement. It also securely connects networks, locations, clouds, and data centers. Additionally, it analyzes and enforces security policies on inbound and outbound traffic between the cloud and the internet.

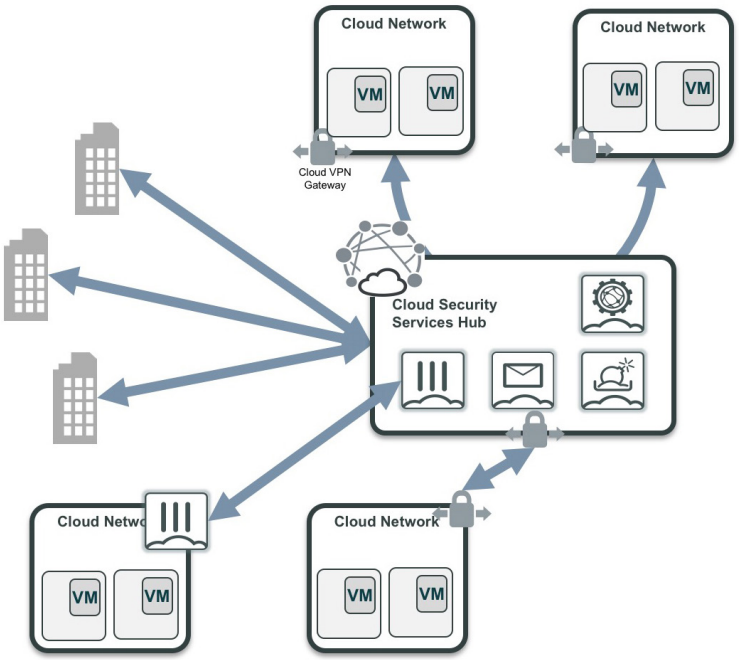


Figure 15: Fortinet acts as a single point of control across clouds and data centers.

### Secure Remote Access

Organizations need global, on-demand, secure access to cloud resources that can incorporate sophisticated access control, event tracking, and analytics. Traditional remote access VPNs, however, cannot meet these requirements.

Security teams need configuration templates that enable secure remote access termination in the cloud. Then, they can dynamically provision FortiGate VM instances that are preconfigured with these templates globally. This enables mobile workforces, customers, and business partners to connect to the virtual organization network. It also connects the cloud network to business applications through VPN tunnels, whether deployed in the cloud or on-premises.

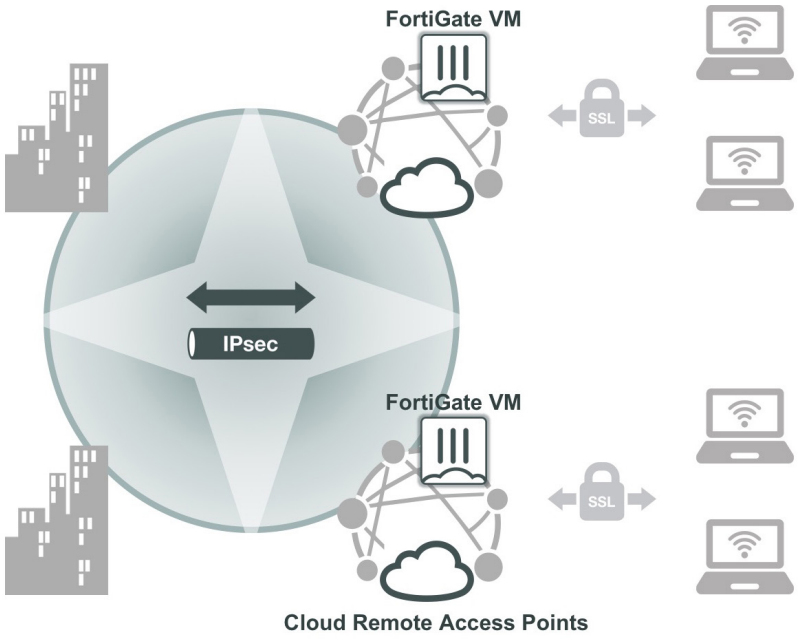


Figure 16: Fortinet acts as a single point of control across clouds and data centers.

## Conclusion

The cloud offers organizations immense business opportunities. But without the right security infrastructure and operational framework in place, the cloud presents serious security challenges that can have far-reaching repercussions. Business-critical applications and data are scattered across multiple clouds. The rapid, decentralized adoption of cloud services often results with a heterogeneous set of security tools and policies that are managed in individual silos.

The shared responsibility model for cloud security dictates that cloud providers only protect the infrastructure and not the applications deployed and running on and data stored in the cloud. Rather, end-users are responsible for securing the application layer. With each cloud provider using different tools and approaching security differently, this creates additional complexity for enterprises that must connect those into the security tools they employ to protect their applications.

To secure multi-cloud environments, enterprises must follow three principles:

- Native integration with all major cloud providers
- A broad suite of security tools that cover the entire attack surface
- Centralized management of security, including automation of workflows and threat-intelligence sharing

Due to the heterogeneity of cloud deployments, there are multiple security use cases that organizations must consider. Each of these comes with security requirements such as integration of all security elements across the entire attack surface, security automation that extends across multiple clouds, cloud-specific security frameworks with centralized policy management for regulatory compliance, security that stretches across the full application life cycle, a cloud services hub for delivering security services, and more.

[1] "Q3 2017 Threat Landscape Report," Fortinet, November 17, 2017.

[2] "FortiGate: Secure SD-WAN," Fortinet, 2019.

[3] "Cloud Business Email Market, 2018-2022," The Radicati Group, Inc., June 2018.





December 16, 2019 3:56 PM

471739-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:Public-Cloud-Strategies-Brief:public-cloud-strategies-brief-121619-343pm