
FORTINET
amazon
web services
Automated,
Unified Security
for Your Entire
IT Environment

CONTENTS

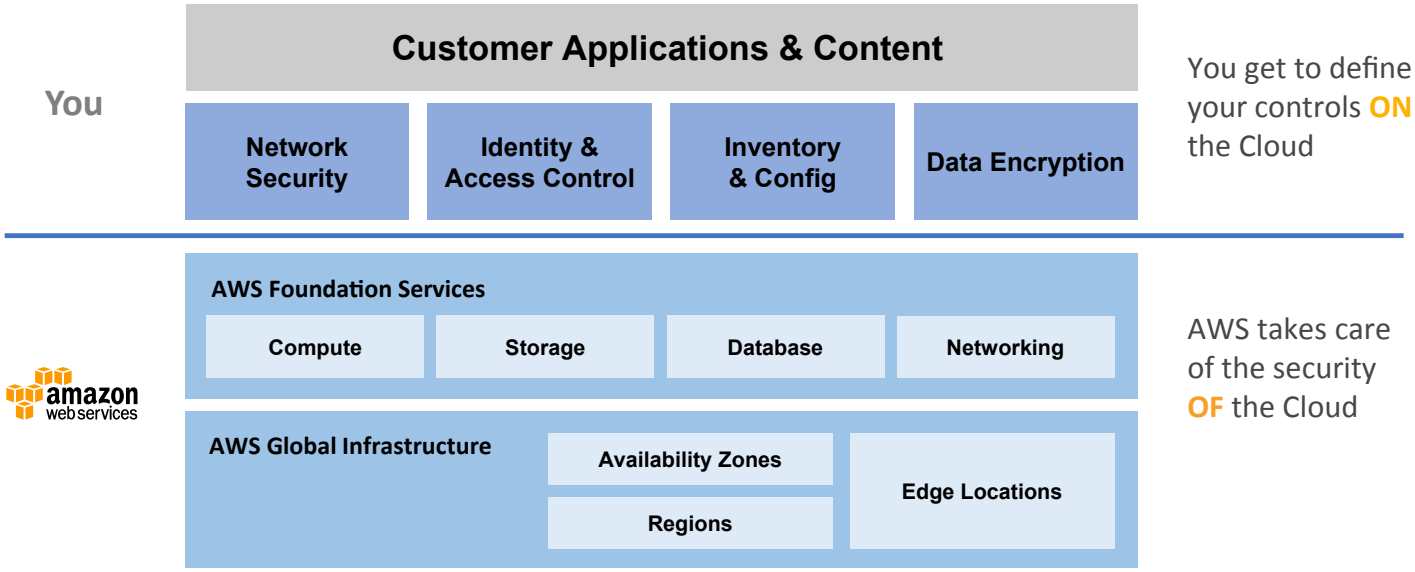
FORTINET EBOOK

SECURITY WITHOUT COMPROMISE

While the Amazon Web Services (AWS) Cloud provides a wide variety of security tools to keep data safe, organizations that don't completely transition to a cloud environment often have questions about how to maintain a unified security posture across both Cloud and on-premises. Whether your data and applications are living in the AWS Cloud, a Hybrid AWS and Private Cloud environment, or any other combination of Hybrid Cloud environment, it is key to protect your entire environment from today's threats.

Most security products designed for legacy on-premises data centers are unable to keep up with the rapid pace of innovation required by today's businesses. It is possible, however, to achieve the level of security your organization needs. According to the recent IDC whitepaper, Assessing the Risk: Yes, the Cloud Can Be More Secure, you can actually achieve greater security in the AWS Cloud than on-premises. Fortinet can help you achieve this with its demonstrated commitment to AWS and host of products designed to keep your cloud-based workloads secure.

AWS SHARED RESPONSIBILITY MODEL



In the AWS Shared Responsibility Model, security is a collaborative effort between AWS and the customer. While AWS provides the secure infrastructure and services for you to develop and run your workloads, you must work to secure the application and data stack. This method allows you to manage everything you put on the Cloud, such as applications and data, by applying security policies to the workloads. It is also up to you to ensure internal policies are met as well as compliance requirements for your specific workloads, such as PCI DSS, SOC2, HIPAA/HITECH, and FISMA.

FORTINET FOR AWS

COMPREHENSIVE SECURITY FOR AWS WORKLOADS

Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. Fortinet provides additional security solutions beyond native security groups which are supported by FortiGuard Labs — Fortinet's team of global researchers dedicated to finding and mitigating the latest IT threats.

The Fortinet Security Fabric creates a unified security posture across your cloud deployments and helps satisfy your part of the AWS Shared Responsibility Model. In proving their commitment to AWS, Fortinet is a certified Advanced Technology Partner in the AWS Partner Network (APN). AWS provides customers with the ability to rapidly scale and innovate while maintaining a secure environment. Your organization can leverage a pay-as-you-go pricing model, meaning that you can achieve the security you need, but without an upfront infrastructure investment, and at a lower cost than in an on-premises environment. AWS and APN Partner Fortinet both provide security options built to keep up with the pace of innovation in modern IT.

Fortinet also provides a host of products to suit your needs, all of which are on AWS Marketplace. Fortinet's strategic integration with AWS enables you to achieve increased throughput, plus gain security elasticity and high availability.

Fortinet products on AWS allow for a flexible and agile deployment where you can either purchase Fortinet products on-demand for your Cloud environment using Pay-As-You-Go pricing or Bring-Your-Own-License (BYOL). Auto scaling for better cloud capacity planning through the AWS CloudFormation deployment template is also available on AWS Marketplace.

WHY FORTINET?

WHY FORTINET?

Fortinet provides security solutions for network, endpoint, application, data center, cloud, and access designed to work together as an integrated and collaborative security fabric. Additionally, Fortinet delivers a complete certified network security products surrounding firewall, intrusion prevention (IPS), antivirus, application control, WAN optimization, data loss prevention (DLP), web filtering, anti-spam filtering, explicit proxy, and log analytics in AWS.

FORTINET ALSO HELPS ENHANCE YOUR CLOUD WORKLOAD SECURITY EXPERIENCE WITH:

- **Cloud Security Automation** – Fortinet provides you with auto scaling to automate your security with efficient capacity planning, including automating route table changes in the event of an instance failure.
- **Hybrid Cloud Migration** – Because Fortinet is designed to help customers unify their security postures across their on-premises and cloud workloads, it is an ideal security platform for those who are looking to migrate from on-premises to a Hybrid Cloud environment, or from a Hybrid Cloud to a full AWS Cloud environment. No matter the makeup of your IT environment, Fortinet can help you maintain the same level of security across all of your components.
- **Cloud Compliance** – Fortinet features a scalable, open, and aware security fabric through its FortiOS. FortiOS can help you consolidate complete cloud compliance reporting by providing a view of compliant and non-compliant security systems and processes, which are regularly tested under Fortinet Best Practice controls.

FORTINET SOLUTIONS FOR AWS

Fortinet's end-to-end security fabric features solutions that are scalable, aware, and actionable. Fortinet solutions use Fortinet Fabric Ready™ Open APIs to gain data center threat visibility to identify anomalous behavior and help de-duplicate threat feed data.

END-TO-END SECURITY FABRIC

- **Scalable** – The fabric can be leveraged to protect your whole IT environment, from your web-based applications to the AWS Cloud, and can easily scale up and down as your workloads demand.
- **Secure** – Besides being backed by a team of 200+ dedicated threat researchers, Fortinet's security solutions share global and local threat intelligence and mitigation information between products for faster protection.
- **Aware** – The security fabric behaves as a single entity regarding policy and logging, enabling end-to-end segmentation for better protection against advanced threats.
- **Actionable** – Fortinet leverages big data cloud systems to correlate threat and network data in order to deliver real-time, actionable threat intelligence.
- **Open** – Gain additional end-to-end security by leveraging well-defined, partner-ready open API extensibility.
- **Compliant** – FortiOS helps consolidate AWS compliance reporting by providing a view of compliant and non-compliant security systems and processes, which are regularly tested under Fortinet Best Practice controls.

API TO CLOUD EXTENSIBILITY

Fortinet security solutions feature open API extensibility to enable organizations to scale and segment cloud instances. It further automates and orchestrates cloud integration and management. By leveraging Fortinet's partner-ready APIs, organizations are able to easily plug in services by Fortinet partners to customize and automate their cloud security to best fit their unique organizational needs.

Fortinet Solutions for AWS

Fortinet also features a complete security portfolio to protect your whole stack and supports both BYOL and On-Demand licensing:

- **Cloud Security Reference Architecture** – Fortinet offers reference architectures that can help you deploy a secure, scalable environment with High Availability (HA) quickly and easily.
- **Auto Scaling Configuration & Deployment** – Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling ensures you have the correct number of compute instances available to handle your applications load. With AWS and Fortinet, you can create Auto Scaling groups and specify the minimum/maximum number of FortiGate security instances in each group.

- **High Availability Configuration & Deployment** – Fortinet helps maintain high availability for your AWS Cloud workloads by offering a shell script that can automate the process of switching between an active and passive firewall if the active firewall is unable to process traffic.
- **Layered Security for East-West Micro-Segmentation** – You can create additional layers of security by directing all traffic for a given subnet within an Amazon Virtual Private Cloud (Amazon VPC) through FortiGate, allowing you to create micro-segmentation within an Amazon VPC.
- **Geo-Distributed Cloud Security Design** – Fortinet maximizes uptime in case of instance failure, a redundant workload in a second Availability Zone should be maintained.
- **Intra-VPC Communication** – With AWS, you can easily establish Amazon VPC peering connections to create a direct east-west networking connection between two Amazon VPCs. Alternatively, if you want to control the segmentation of your Amazon VPCs, you can create separate Amazon VPCs and route traffic between them.

ABOUT FORTINET:

Fortinet secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. More than 270,000 customers worldwide trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

ABOUT AWS:

For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 70 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 33 Availability Zones (AZs) across 12 geographic regions in the U.S., Australia, Brazil, China, Germany, Ireland, Japan, Korea, and Singapore. AWS services are trusted by more than a million active customers around the world – including the fastest growing startups, largest enterprises, and leading government agencies – to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit http://aws.amazon.com.