Key Steps to Optimizing Cloud Security

Elevating security on AWS using Fortinet application-level visibility

Table of Contents

Do you know what's missing from your cloud security strategy?

There's no question that moving to the cloud makes it easier for your business to continue innovating and stay agile. However, migrating your security practice to the cloud can feel like a lot to navigate on your own. As your digital surface expands, it becomes increasingly more important to understand your options for managing security across your ecosystem and mitigating risk.

Wouldn't it be nice if someone told you what your cloud security strategy was missing? Fortinet has teamed up with Amazon Web Services (AWS) to help you embrace the cloud with confidence. Using the AWS Shared Responsibility Model, Fortinet can help you identify potential gaps in your environment and your skill set. Fortinet provides industry-leading security solutions and services designed and built to run industry-leading cloud services.

Introducing cloud into your IT environment can raise some big questions about security that Fortinet and AWS can help you answer with confidence.

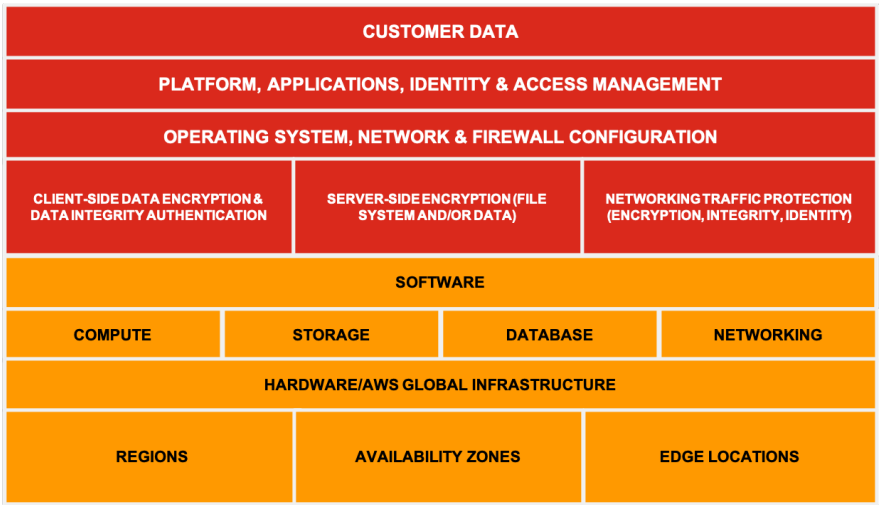
"Can we take our on-prem security practices with us?"

"How do I know if my cloud environment is secure?"

Delivering security in the cloud requires close collaboration

The AWS Shared Responsibility Model provides a framework that defines your role in cloud security. AWS handles the security OF the cloud, which includes securing the hardware, software, and networking that run your workloads. As a customer of AWS, you are responsible for the security IN the cloud, which gives you full autonomy about which policies and services are right for your specific systems and data.

Security IN the cloud



Security OF the cloud

Fortinet collaborates with AWS to develop comprehensive security configurations that make it easier for you to implement AWS best practices in the cloud.

The partnership between Fortinet and AWS is a better-together combination that ensures your workloads on AWS are protected by best-in-class security solutions powered by comprehensive threat intelligence and more than 20 years of cybersecurity experience. Integrations with key AWS services simplify security management and enable automation, ensure full visibility across environments, and provide broad protection across your workloads and applications.

Whether you're expanding your AWS footprint, securing hybrid-cloud assets, or currently migrating to AWS, Fortinet Security Fabric delivers security-driven networking and adaptive cloud protection for the ultimate flexibility and control you need to build in the cloud.

FortiGuard Labs integrates premium protection into Fortinet Security Fabric

FortiGuard Labs is at the heart of the company's culture of innovation. The research and development (R&D) investments have yielded over 700 technology patents that demonstrate the commitment to keeping you on the leading edge of security with solutions you can trust.

Fortinet uses real-time intelligence gained through bi-directional Fortinet Distribution Network in FortiGuard Labs to continuously update the Fortinet Security Fabric.

Every day, the platform ingests over 100 billion security events and applies artificial intelligence and machine learning to understand, classify, and develop effective responses to in-the-wild malware—making changes to the fabric every few hours.

Updates to the Fortinet Security Fabric flow seamlessly to the AWS services it integrates with such as; Amazon GuardDuty, AWS Outposts, AWS Transit Gateway, AWS Gateway Load Balancer, Amazon EC2, Amazon CloudFront, AWS WAF, AWS Network Firewall, and more. Running Fortinet and AWS, you can be sure your environment is optimized for the most recent insights in threat intelligence.

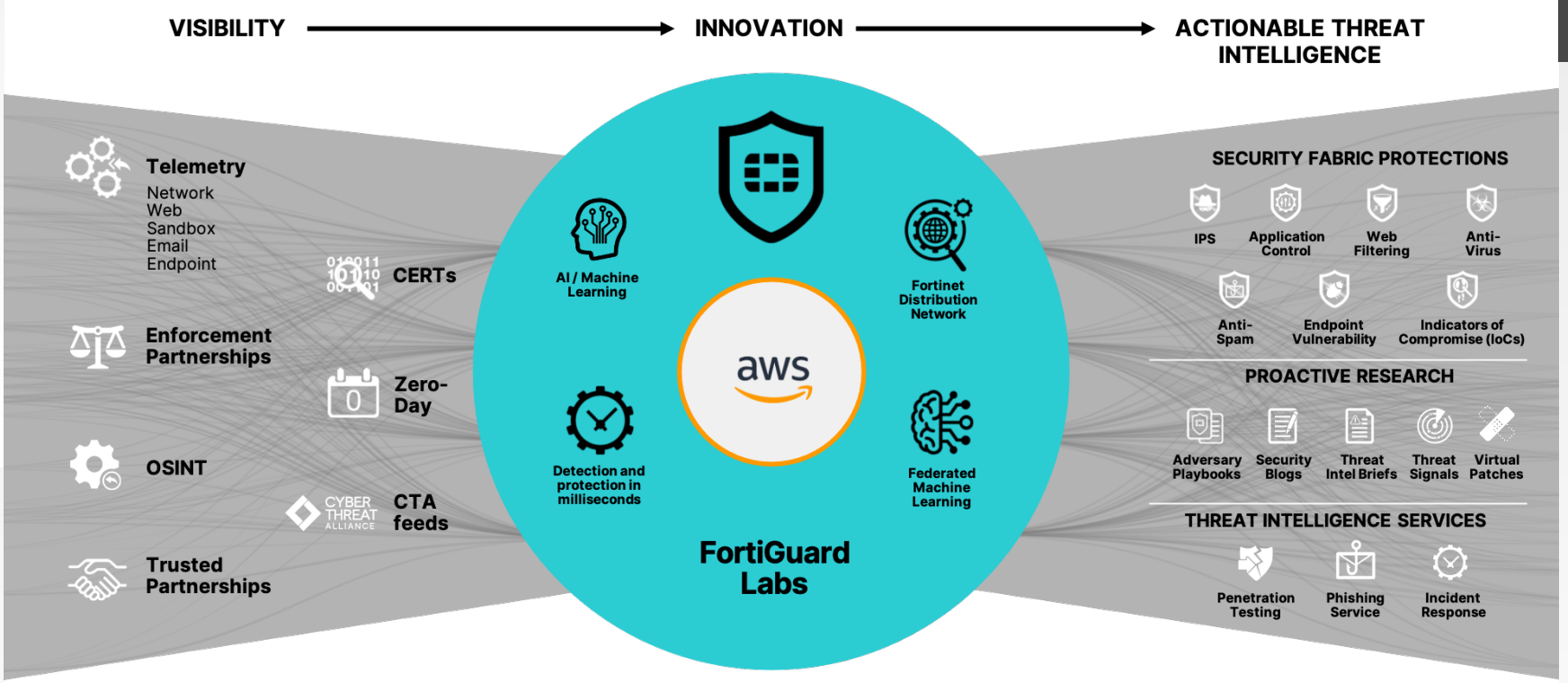
340+ thousand malware programs neutralized per minute

18 million network intrusion attempts resisted per minute

1 billion security updates produced every day

FortiGuard Labs
Global threat research and response

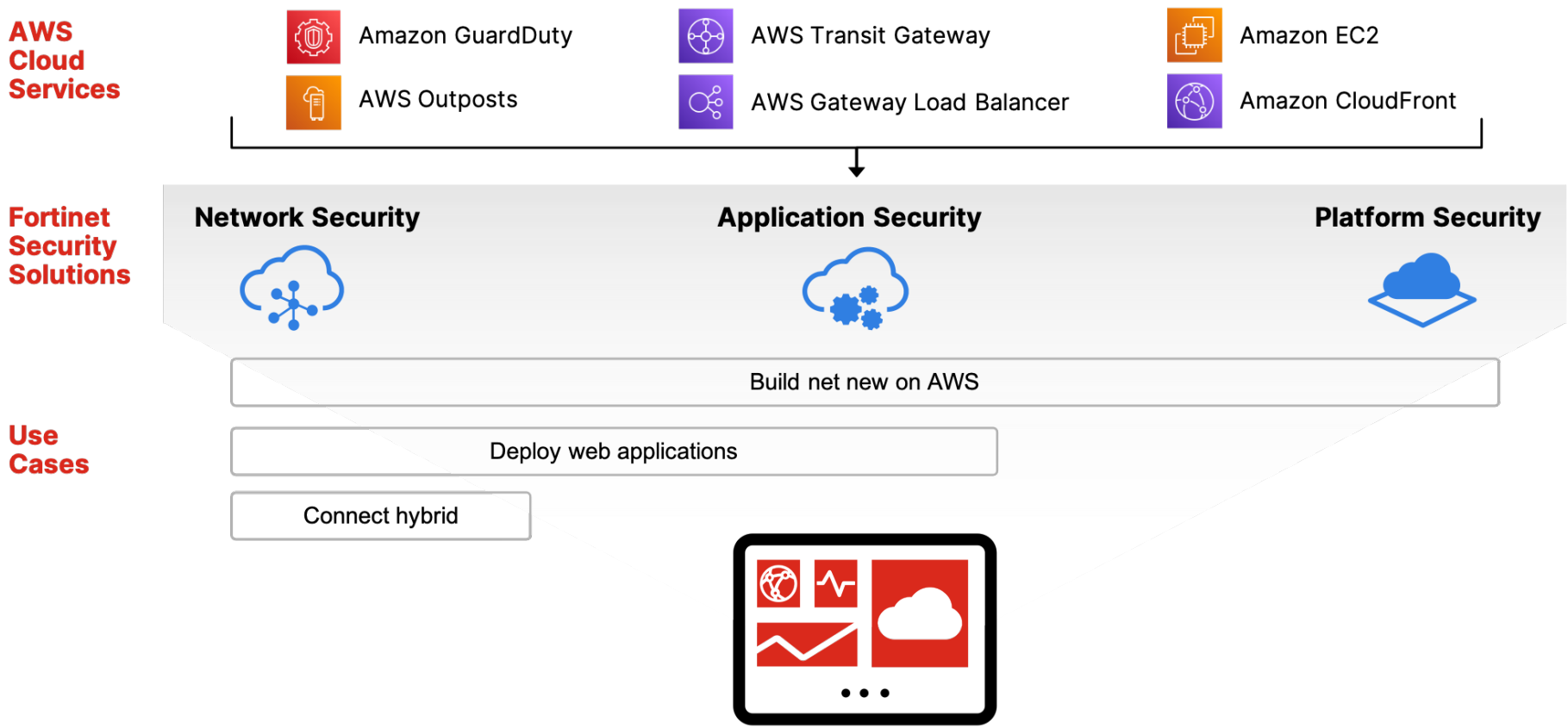
Get real-time visibility into threats with FortiGuard Labs



Learn more about FortiGuard Labs

End-to-end visibility into every type of workload on AWS

Fortinet offers network, application, and platform security solutions that integrate with AWS to provide comprehensive threat protection. It makes all your security data visible and actionable through single-pane-of-glass management and security automation. The comprehensive management view helps you streamline operations, ensure policy consistency, and unify your workflows across different types of workloads—from those you build net new on AWS to those you lift and shift straight out of your datacenter.



Experience unified policy control and end-to-end visibility across all your assets and use cases with Fortinet and AWS

Build net-new on AWS

Whether you want to securely access AWS infrastructure or build net-new applications on AWS, Fortinet provides a broad set of natively integrated security solutions for full visibility, advanced threat defense, and centralized management in the cloud. With Fortinet and AWS, you can start every new cloud-based project confident your security strategy will grow with you.

Enhance AWS Network Firewall protection of your **Amazon Virtual Private Clouds** (Amazon VPC) using **Fortinet Managed IPS Rules** for simple-to-deploy, predefined intrusion protection policies that address common attack scenarios.

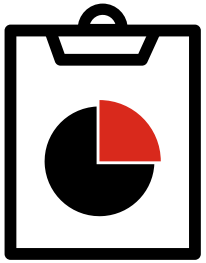
Establish more robust security controls with AWS WAF without adding management or architectural complexity using **Fortinet Managed WAF rulesets for AWS WAF**, which are based on FortiWeb WAF security service signatures and updated with insights from FortiGuard Labs.

Secure your Amazon VPC environments while improving high availability and scaling using FortiGate-VM Next Generation Firewall integration with **AWS Gateway Load Balancer** to help with automation.

Enhance AWS Network Firewall protection	Establish more robust security controls with AWS WAF	Secure your Amazon VPC environments, improve high availability and scaling
Fortinet Managed IPS Rules	Fortinet Managed WAF rulesets for AWS WAF	FortiGate-VM Next Generation Firewall
+	+	+
Amazon Network Firewall	Amazon WAF	AWS Gateway Load Balancer

"We needed high-end security capabilities even though we weren't an enterprise-scale company. Fortinet was able to deliver a solution, based on AWS, to boost our size and supplement our in-house staff."

— Eddie Tse, Deputy Chief Technology Officer, WeLab Bank



Fortinet Cloud Security Advisory & Consulting Services

Create a blueprint for designing and implementing advanced security across your AWS environments, network, and applications. Fortinet consulting services offers security assessments of your AWS deployments to enhance your overall security posture and remediate any existing misconfigurations.

Deploy web applications

Deploying applications in the cloud creates a new attack surface, with exposure to the public internet that enables user connections from unmanaged devices over networks the organization doesn't control. While many organizations have adopted DevOps practices, DevOps teams are often responsible for securing cloud applications but may lack security expertise. Fortinet can help you add web application security without slowing down your developers.

Unlock additional security controls for web apps and APIs with the cloud-based SaaS web application firewall (WAF) by Fortinet. **FortiWeb Cloud WAF-as-a-Service** uses machine learning to protect public cloud-hosted web applications from the OWASP Top Ten, zero-day threats, and other application-layer attacks. It requires no hardware or software, colonies of FortiWeb WAF gateways run in most AWS regions and enable organizations to scrub application traffic within the same region their applications reside, addressing performance and regulation concerns, as well as keeping traffic cost to a minimum. FortiWeb is also available as a VM for IaaS deployments.

Enable robust security controls on AWS with latest in threat protection without adding management or architectural complexity. **Fortinet Managed Rules for AWS WAF** are based on FortiWeb WAF security service signatures and updated with insights from FortiGuard Labs.

Enable robust security controls AWS with the latest threat intelligence

Fortinet Managed Rules for AWS WAF

+

Amazon WAF

Unlock additional security controls for web apps and APIs leveraging ML

FortiWeb Cloud WAF-as-a-Service

Migrate and connect hybrid solutions

Hybrid cloud deployments that unite on-premises datacenters and workloads on AWS provide much needed flexibility for organizations to modernize and innovate across environments. But security across these extended environments tends to be inconsistently enforced and complex to manage.

Strengthen your security posture for migration or hybrid use cases through natively integrated security functionality that works across AWS services such as **Amazon GuardDuty**, **AWS Security Hub**, and **AWS Outposts**. **Fortinet Adaptive Cloud Security solutions** and **Security Fabric** deliver comprehensive visibility and protection through the Shared Responsibility Model—from on-premises to the AWS Cloud.

Get robust, secure connectivity to Amazon VPCs and for hybrid-cloud deployments with **FortiGate Next-Generation Firewalls** (NGFWs). Ensure centralized, consistent security policy enforcement and application-centric, resilient connectivity through a high-performance VPN or SD-WAN architecture that helps with network segmentation, and application security.

Simplify security management across hybrid environments with **FortiManager**, which provides single-pane-of-glass management across the entire extended enterprise—including Fortinet NGFWs, switches, wireless infrastructure, and endpoints.

Simplify compliance reporting and tasks using **FortiAnalyzer** to analyze, report, and archive security events, network traffic, web content, and messaging data.

"By creating a Cloud Security Services Hub within each region and having the FortiGate VM firewalls secure traffic across Amazon VPCs (east-west traffic) consistently across our on-premises and cloud infrastructures, we can address business needs in a much more timely and effective manner while maintaining consistent security posture."

— Anish John, Cloud Network Architect, Autodesk

Strengthen your security posture for migration or hybrid uses

Fortinet Security Fabric and adaptive cloud security solutions

+

Amazon GuardDuty

AWS Security Hub

AWS Outposts

Get robust, secure connectivity to Amazon VPCs and for hybrid-cloud deployments

FortiGate-VM Next Generation Firewall

+

AWS Gateway Load Balancer

Simplify security management across hybrid environments

FortiManager

Simplify compliance reporting and tasks

FortiAnalyzer

Fortinet and AWS: Leaders in cybersecurity

Founded in 2000, Fortinet is a top cybersecurity company in the world. Fortinet has been placed in six Gartner Magic Quadrants, and 2020 marked the 11th time in a row that Fortinet was named a leader in network firewalls.

Fortinet is a trusted AWS Security Partner with critical experience. It serves more than 500,000 customers, protecting data on premises and in the cloud. Fortinet protects 70 percent of Fortune 100 companies and is the most deployed network security solution in the world.

Established APN partner

aws partner network

Advanced
Technology
Partner

Security Competency

Networking Competency

Marketplace Seller

11 years running as a leader in network firewalls

Garnering more third-party validation than anyone else

Gartner peerinsights customers' choice™

FORTINET RECOMMENDED · AV comparatives · virus BULLETIN · ICSA labs CERTIFIED

*The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

Find the right Fortinet security solution for your workload

AWS Marketplace enables full software lifecycle management for all your Fortinet solutions, making it easy for you to access, deploy, and onboard our suite of security services. Discover the broad range of Fortinet Adaptive Cloud Security solutions available in multiple consumption models—virtual machine, container, and SaaS form factors—with bring-your-own-license and pay-as-you-go billing options.

Free Trial

Get started in AWS Marketplace with a free trial

Ideal for initial evaluation

Hourly

Pay for software and compute capacity by the hour, with no long-term commitments

Ideal for development and testing, or workloads with inconsistent traffic

Monthly

Make a monthly payment, and receive a discount on the monthly pricing charge

Ideal for temporary projects and baseline workloads

Annual and multi-year

Make a one-time payment, and receive a significant discount

Multi-year options are also available

Ideal for long-term workloads

BYOL

Migrate to AWS with your existing product licenses

Intended for pre-existing customers

Private Offers

Negotiate a custom price with a software seller

Offer is reviewed and accepted in AWS Marketplace

Ideal for high-value and complicated transactions

To learn more about Fortinet and AWS, visit www.fortinet.com/aws or get started with a free trial on AWS Marketplace.

To get the conversation started with one of our security experts, reach out to awssales@fortinet.com.

www.fortinet.com

July 20, 2021 5:34 PM

Fortinet_AWS_B2G_ebook_DESIGN_07202021

123456-0-0-EN