Evolve Your Cloud Security on AWS

Protect Your Applications with Cloud-Native Visibility and Control

<table>
<thead>
<tr>
<th>Overview</th>
<th>Use Cases</th>
<th>Why AWS and Fortinet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Fabric</td>
<td>End-to-end Visibility</td>
<td>Hybrid-Cloud Security</td>
</tr>
<tr>
<td>Web Application &amp; API Protection</td>
<td>Risk Management &amp; Visibility</td>
<td>Zero Trust Network Access</td>
</tr>
<tr>
<td>Cloud Consulting</td>
<td>AWS Marketplace</td>
<td></td>
</tr>
</tbody>
</table>
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?
Best-in-class Security Requires an Integrated Approach

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.

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, applications, and containers.

Whether you’re expanding your AWS footprint, securing hybrid-cloud assets, or currently migrating to AWS, Fortinet Security Fabric delivers secure networking and adaptive cloud protection for the ultimate flexibility and control you need to build in the cloud.
Fortinet’s Security Fabric Delivers AI and ML-based Protection on AWS

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
Gain End-to-End to Visibility and Control Across Workloads

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 data center.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefits</td>
<td>Centralized visibility, control, and automation simplified</td>
<td>Protect against OWASP Top 10 threats, zero-day, and other app layer attacks</td>
<td>Manage cloud risks with actionable insights</td>
<td>Zero trust network access</td>
</tr>
<tr>
<td>Fortinet Solutions</td>
<td>FortiGate Cloud-Native Firewall (CNF)</td>
<td>FortiWeb Cloud WAF-as-a-Service</td>
<td>Fortinet Managed Rules</td>
<td>Fortinet Zero Trust Access</td>
</tr>
<tr>
<td></td>
<td>FortiGate-VM</td>
<td>FortiWeb Cloud WAF-as-a-Service</td>
<td>FortiCNP Cloud Native Protection</td>
<td>Fortinet ZTNA Application Gateway</td>
</tr>
<tr>
<td>AWS Integrations</td>
<td>AWS Firewall Manager</td>
<td>Gateway Load Balancer</td>
<td>AWS WAF</td>
<td>AWS Security Hub</td>
</tr>
<tr>
<td></td>
<td>AWS Firewall Manager</td>
<td>Gateway Load Balancer</td>
<td>AWS WAF</td>
<td>Amazon GuardDuty</td>
</tr>
<tr>
<td></td>
<td>AWS Firewall Manager</td>
<td>Gateway Load Balancer</td>
<td>AWS WAF</td>
<td>Amazon Inspector</td>
</tr>
<tr>
<td></td>
<td>AWS Firewall Manager</td>
<td>Gateway Load Balancer</td>
<td>AWS WAF</td>
<td>AWS Gateway Load Balancer</td>
</tr>
</tbody>
</table>

Overview

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud Consulting</td>
</tr>
</tbody>
</table>

Use Cases

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>Why AWS and Fortinet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid-Cloud Security</td>
<td>Cloud Consulting</td>
</tr>
<tr>
<td>Web Application &amp; API Protection</td>
<td>AWS Marketplace</td>
</tr>
<tr>
<td>Risk Management &amp; Visibility</td>
<td>Cloud Consulting</td>
</tr>
<tr>
<td>Zero Trust Network Access</td>
<td>AWS Marketplace</td>
</tr>
</tbody>
</table>
Use Case: **Hybrid Cloud Security, Natively Delivered**

Retain consistent protection and visibility across distributed environments

**Fortinet Security Fabric**

- **Advanced Threat Protection**
  FortiGate Next-Generation Firewalls (NGFWs) provide secure connectivity/SD-WAN, network segmentation, and application security for hybrid-cloud-based deployments.

- **Threat Intelligence**
  The Fortinet Security Fabric integrates the latest AI-driven threat intelligence from our in-house research group, FortiGuard Labs.

- **Zero Operations Overhead**
  FortiAnalyzer allows you to analyze, report, and archive security events, network traffic, web content, and messaging data to help simplify compliance tasks.

- **Simplified Security Management**
  FortiManager provides single-pane-of-glass management across the entire extended enterprise.

**Hybrid cloud deployments** that unite on-premises data centers 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.
**Use Case: Hybrid Cloud Security, Natively Delivered**

**Strengthen your security posture for hybrid-cloud use cases** through natively-integrated security functionality that works across AWS services such as Amazon GuardDuty, AWS Security Hub, and AWS Outposts. Fortinet Cloud Security solutions and Security Fabric deliver comprehensive visibility and protection—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 and modernize your network protection on AWS with FortiGate Cloud Native Firewall (CNF). This firewall-as-a-service removes security infrastructure overhead, while providing IPS, anti-malware, advanced filtering, application-layer visibility, and more. FortiGate CNF integrates with AWS services to reduce operational complexity and scale security seamlessly.

**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
Use Case: **Web Application & API Protection**

Deploying a web application firewall (WAF) is the cornerstone of comprehensive security for web apps and APIs. WAFs use a combination of rules, threat intelligence, and heuristic analysis of traffic to ensure that malicious traffic is detected and blocked before reaching web applications.

**FortiWeb Cloud WAF-as-a-Service**

- **Web Application Security**: Protect against known and unknown threats including the OWASP Top 10.
- **Bot Mitigation**: Block the full range of malicious bot activity (e.g., content scraping, denial of service, data harvesting, transaction fraud).
- **Easy to Deploy**: With a built-in setup wizard and predefined policies, deploy in just minutes and start protecting your apps from threats.
- **API Security**: Protect the APIs that enable B2B communication and support your mobile applications.
- **Machine Learning**: Protect your web apps and APIs while reducing management overhead.

**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.

**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 10, zero-day threats, and other application-layer attacks.

Requiring 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 costs to a minimum. FortiWeb is also available as a VM for IaaS deployments.
Use Case: **Risk Management & Visibility**

Central to a strong security posture is proactive risk management. By focusing on risk prioritization, mitigation, and remediation, you can bolster your protection against threats. Fortinet solutions deliver visibility into your infrastructure, workloads, and applications on AWS, to help reduce risk in cloud environments.

**FortiCNP**, Fortinet’s cloud-native protection product, simplifies and streamlines cloud security operations. Its patented Resource Risk Insights (RRI) technology correlates and contextualizes security findings from AWS security services and Fortinet security products. This way, you can maximize the value of your AWS cloud security services, including Amazon GuardDuty, Amazon Inspector, AWS Security Hub, AWS CloudTrail, and AWS Organizations. FortiCNP calculates risk and stacks ranks the highest-risk resources based on analysis of the security posture, vulnerabilities, permissions, and threat signals.
Use Case: Zero Trust Network Access

To protect networks and applications, Fortinet solutions can help you implement a zero-trust access approach and provide the least access privileges. Implementing zero-trust access includes requiring strong authentication capabilities, powerful network access control tools, and pervasive application access policies.

Fortinet Zero Trust Access continually verifies who and what is using your AWS resources. IoT and endpoint devices are identified and secured, while IT teams gain full visibility into and control over what's connected to your network.

Fortinet ZTNA Application Gateway makes it simple to provide granular application control for users with consistent policies regardless of where they connect from. ZTNA Application Gateway provides consistent ZTNA enforcement for both remote and campus workers. Fortinet ZTNA Application Gateway integrates seamlessly with FortiClient to provide robust security controls such as user identity checks and posture checks before allowing the users access to an application.

Wherever the user is
Verified user identity, device identity, and posture check prior to access

Campus
Branch
Remote

Wherever the application is
SaaS Apps
aws
Data Center

OS
Founded in 2000, Fortinet is a top cybersecurity company in the world. Fortinet has been placed in six Gartner Magic Quadrants, and 2022 marked the 13th 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 635,000 customers, protecting data on premises and in the cloud. Fortinet leverages all its critical insights, experience, and know-how gained over the past two decades to bring you security engineered for the cloud, ensuring your workloads on AWS stay secure, scalable, and resilient.
Design a Path to an Enhanced Cloud Security Posture

To stay ahead of the rapidly evolving threat landscape, organizations must adopt a cloud security architecture and operations that include a comprehensive and measured approach to cybersecurity. Fortinet can help you discover, align, and guide your organization through the cloud-enablement journey. Fortinet consulting services offers security assessments of your AWS deployments to enhance your overall security posture and remediate any existing misconfigurations.

“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
Easily Deploy Fortinet Security Solutions via AWS Marketplace

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.

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.

Get started in AWS Marketplace with a free trial
Ideal for initial evaluation

Pay for software and compute capacity by the hour, with no long-term commitments
Ideal for development and testing, or workloads with inconsistent traffic

Make a monthly payment and receive a discount on the monthly price charge
Ideal for temporary projects and baseline workloads

Make a one-time payment and receive a significant discount
Multi-year options are also available
Ideal for long-term workloads

Migrate to AWS with your existing product licenses
Intended for pre-existing customers

Negotiate custom price with a software seller
Offer is reviewed and accepted in AWS Marketplace
Ideal for high-value and complicated transactions