Evolve Your Cloud Security on AWS

Protect Your Applications and APIs with Cloud-Native Visibility and Control
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 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 identify potential gaps in your environment and your skill set using the **AWS Shared Responsibility Model**. Fortinet security solutions and services are designed and built to secure your application and workloads across your cloud or hybrid environments.

Expanding your cloud footprint 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?"

"Do we have what it takes to bridge the gaps?"

The priorities may seem clear, but the barriers are plenty. A clear strategy, vision, and plan to work through them, however, can securely realize the benefits your business desires from cloud transformation.

**TOP CLOUD security priorities**
- 51% Preventing cloud misconfigurations
- 48% Securing major cloud apps already in use
- 43% Defending against malware
- 39% Reaching regulatory compliance

**TOP GAPS blocking success**
- 37% Lack of staff resources or expertise
- 30% Legal and regulatory compliance
- 29% Data security, loss, and leakage risks
- 27% Integration with existing IT environment

**BENEFITS realized**
- 53% More flexible capacity and scalability
- 45% Increased agility
- 44% Improved availability and business continuity
- 41% Accelerated deployment and provisioning

Source: Fortinet, 2023 Cloud Security Report
Best-in-Class Security Outcomes Require 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
- Enable automation
- Ensure full visibility across environments
- 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. Research and development investments have yielded over 700 technology patents that demonstrate our commitment to keeping you on the leading edge of security with solutions you can trust.

Fortinet uses real-time intelligence gained through the 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 over the AWS services it integrates with, including Amazon GuardDuty, AWS Outposts, AWS Transit Gateway, AWS Gateway Load Balancer, Amazon CloudFront, AWS WAF, and more. By running Fortinet with AWS, you can be sure your environment is protected with 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 Visibility and Control Across Workloads and Use Cases

Fortinet brings together network, application, and platform security solutions that integrate with AWS to provide comprehensive visibility and protection. 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 Firewall Manager. The integrated single-plane-of-glass management 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>Enforce ZTNA policies for both remote workers and on-campus workers</td>
</tr>
<tr>
<td>Fortinet Solutions</td>
<td>FortiGate Cloud-Native Firewall (CNF)</td>
<td>FortiWeb WAF-as-a-Service</td>
<td>Fortinet Managed Rules</td>
<td>FortiCNP Cloud Native Protection</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, Amazon GuardDuty, Amazon Inspector</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overview</th>
<th>Use Cases</th>
<th>Why AWS and Fortinet</th>
</tr>
</thead>
</table>
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**: Integrations with key AWS services provide automated and scalable protection.
- **Compliance Reporting**: 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.

Use Case: **Hybrid Cloud Security, Natively Delivered**

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.

**Fortinet Cloud Security** solutions and Security Fabric deliver comprehensive visibility and protection—from on-premises to the AWS Cloud.

<table>
<thead>
<tr>
<th>Overview</th>
<th>Use Cases</th>
<th>Why AWS and Fortinet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intro</td>
<td>Hybrid-Cloud Security</td>
<td>Cloud Consulting</td>
</tr>
<tr>
<td>Security Fabric</td>
<td>Cloud-Native Network Security</td>
<td>AWS Marketplace</td>
</tr>
<tr>
<td>End-to-end Visibility</td>
<td>Web Application &amp; API Protection</td>
<td></td>
</tr>
</tbody>
</table>
**Use Case: Cloud-Native Network Security, Smartly Provisioned**

Simplify and modernize your network protection on AWS for frictionless security at any scale.

**FortiGate CNF**

- **NGFW Protection**: Outbound, inbound, and east-west traffic inspection.
- **Advanced Security**: Artificial intelligence (AI) and machine learning (ML), along with Fortinet’s global threat visibility, help block advanced attacks.
- **Zero Operations Overhead**: Focus only on security-policy management and offload service-infrastructure maintenance to Fortinet.
- **Management Flexibility**: Three management options are available: FortiGate CNF console, AWS Firewall Manager, and FortiManager.
- **Optimized TCO**: Cut down complexity, remove the heavy lifting around network security operations, and apply robust security controls to reduce cyber risk.

Delivery as Software-as-a-Service (SaaS) on AWS offloads the need for security teams to coordinate provisioning and update activities. Integrations with native AWS services deliver scalability and security across multiple AWS accounts.

**FortiGate Cloud Native Firewall (CNF)** firewall-as-a-service removes security infrastructure overhead while providing IPS, anti-malware, advanced filtering, application-layer visibility, and more.
Use Case: **Web Application & API Protection**

Detect and block malicious traffic before it can reach 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.

Web application firewalls (WAFs) are the cornerstone of comprehensive security for web apps and APIs, combined rules, threat intelligence, and heuristic analysis of traffic.

**FortiWeb Cloud WAF-as-a-Service** protects web applications and APIs from OWASP Top 10 threats, zero-day attacks, and other application layer attacks.
Use Case: **Risk Management & Visibility**

Visibility into your infrastructure, workloads, and applications on AWS reduces cloud risk

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.

**FortiCNP** cloud-native protection collects information from AWS security services as well as Fortinet cloud security products to help prioritize risk management activities based on a broad set of security signals from their AWS environments.
Use Case: **Zero Trust Network Access**

Least access privileges require strong authentication capabilities, powerful network access control tools, and pervasive application access policies.

Zero trust access makes it simple to provide granular application control for users with consistent policies regardless of where they connect from.

**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.
Unzer, an innovative, modular platform for international payment transactions, debuted in 2020 after a merger of several acquired companies, including Heidelpay. Unzer facilitates the entire spectrum of payment management—from payment processing to customer analytics to risk management—for retail and ecommerce organizations. As such, data security and compliance with regulations like the payment card industry data security standard (PCI DSS) are paramount. Using solutions from Fortinet, the Unzer security team created the Unzer enterprise network with zero trust network access to protect its workloads on Amazon Web Services (AWS).

“We moved to AWS for its reliability and the agility to launch applications rapidly, so we designed a security architecture with Gateway Load Balancer and Fortinet FortiGate firewalls across different Availability Zones to enable scaling up and down.”

— Hooman Ahmadi, Network Engineering Manager, Unzer
## AWS and Fortinet: A Better-Together Combination

When it comes to effectively managing security risk to optimize ROI, the combination of AWS with Fortinet offers advantages that other solutions are hard-pressed to match. With tools designed to mitigate security risk, improve protection, and reduce complexity, Fortinet Security Fabric solutions leverage capabilities such as threat intelligence, data correlation, automation, AI, and machine learning, which are all designed to interoperate and respond to threats as a single, coordinated system.

The Fortinet FortiGate Next-Generation Firewall (NGFW) combines security and networking services to enable both content and network protection in an Amazon Web Services (AWS) environment. Fortinet designed this solution to inspect traffic as it enters and leaves the network while simultaneously providing integrated security capabilities. With AWS Marketplace’s one-click deployment for enterprise-class IT, you can secure and monitor your cloud-based network and the data and traffic running on it.

> “The Fortinet FortiGate Next-Generation Firewall (NGFW) combines security and networking services to enable both content and network protection in an Amazon Web Services (AWS) environment. Fortinet designed this solution to inspect traffic as it enters and leaves the network while simultaneously providing integrated security capabilities. With AWS Marketplace’s one-click deployment for enterprise-class IT, you can secure and monitor your cloud-based network and the data and traffic running on it.”

— Enterprise Strategy Group
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

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.
Security Engineered for the Cloud

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.

Established APN partner

13 years running as a leader in network firewalls

Garnering more third-party validation than anyone else
Flexible Licensing and Deployment 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.

**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 price 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*

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

**FortiFlex**
Migrate and build securely with dynamic deployment and elastic scalability
Control and reduce cloud spend
*Ideal for those wanting flexibility or looking to drawdown EDP*

---

**Overview**

- Intro
- Security Fabric
- End-to-end Visibility
- Hybrid-Cloud Security
- Cloud-Native Network Security
- Web Application & API Protection
- Risk Management & Visibility
- Zero Trust Network Access
- Cloud Consulting
- AWS Marketplace

**Use Cases**

- Zero Trust Network Access
- Intro
- Security Fabric
- End-to-end Visibility
- Hybrid-Cloud Security
- Cloud-Native Network Security
- Web Application & API Protection
- Risk Management & Visibility
- Zero Trust Network Access
- Cloud Consulting
- AWS Marketplace

**Why AWS and Fortinet**

- Migrate and build securely with dynamic deployment and elastic scalability
- Control and reduce cloud spend
- Ideal for those wanting flexibility or looking to drawdown EDP
# Find Your Path to Enable Innovation with Fortinet and AWS

<table>
<thead>
<tr>
<th>EXPLORE</th>
<th>EXAMINE</th>
<th>EXPERIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations</strong></td>
<td>Program: Usage-based Security Licensing with FortiFlex</td>
<td>eBook: Security Considerations for Your AWS Cloud Migration</td>
</tr>
</tbody>
</table>

To learn more about Fortinet and AWS, visit [www.fortinet.com/aws](http://www.fortinet.com/aws).
To get the conversation started with one of our security experts, reach out to awssales@fortinet.com.
www.fortinet.com/aws