FORTINET

Deliver 360-Degree Protection for Your AWS Environments and Landing Zones

Unify your network, application, and AI workload security with Fortinet and AWS

Table of contents

Understanding AWS security: A reality check

You've established your AWS landing zone and are now deploying workloads with centralized logging, identity and access management, network design, and governance. Your applications are scaling, and you're exploring the possibilities of agentic AI. But as your cloud and AI footprints grow, so does your attack surface, along with the complexity of keeping it all secure.

Today's cloud security is complex

Cloud environments are dynamic by design. Constantly changing networks, workloads, and access patterns mean that traditional security approaches will fall short. AI-enabled applications, agentic deployment, Model Context Protocol (MCP), and LLMs are adding an entirely new category of risks that existing security tools weren't designed to address. Cloud security teams are struggling to keep up with the changes and risks.

As a result, 69% of organizations have reported identity and access-related cloud security incidents in the past twelve months.[1] Most of them are caused by human error, most commonly misconfigurations. Contributing factors to those errors are fragmented visibility, alert fatigue, and security engineers who are stretched thin.[2]

A new approach is imperative

Effective Amazon Web Services (AWS) security requires a unified approach that protects your networks, applications, and AI workloads with consistent policies, centralized visibility, and intelligence that keeps pace with evolving threats.

This ebook shows how Fortinet works with AWS services to deliver that unified approach to all aspects of security, from using the cloud for storage and hosting to using it as a foundation for agentic AI.

Security complexity and concerns by the numbers[1]

81%
of organizations rely on two or more cloud providers to run critical workloads.

66%
lack confidence in their ability to detect and respond to cloud threats in real time.

74%
report an active shortage of cybersecurity talent.

[1] Fortinet 2026 Cloud Security Report

[2] Cloud Complexity Outpacing Human Defenses, Report Warns

Stay ahead of threats with a trusted AWS security ISV protecting cloud and AI workloads at scale

While AWS secures the cloud infrastructure, organizations are responsible for securing what they build and run in it. That's where Fortinet delivers. Fortinet is a trusted AWS Security Partner with Security and Network Competencies, many technical integrations, and more than 42,000 joint AWS customers. Fortinet also supports the AWS European Sovereign and Saudi Kingdom Sovereign clouds for regional compliance requirements. FortiGuard Labs, the dedicated in-house threat intelligence and research organization at Fortinet, is at the core of this trust.

Deep integrations across the AWS ecosystem

The Fortinet Security Fabric connects natively with core AWS services, including AWS Security Hub, Amazon GuardDuty, AWS Transit Gateway, AWS Gateway Load Balancer, and Amazon CloudFront. These validated integrations deliver single-pane-of-glass management, cloud-native visibility, consistent policy enforcement, and security automation across hybrid and multi-cloud deployments. The result is a cohesive operational model that extends baseline AWS security with layered, 360-degree defense-in-depth protection across every account and workload.

Real-time data analysis combined with AI and machine learning deliver threat intelligence

The FortiGuard Labs organization develops and delivers AI-powered security services to protect customers from cyberattacks. Using millions of global sensors, it analyzes real-time data to identify, block, and provide actionable intelligence on malware, ransomware, and zero-day vulnerabilities across the Fortinet Security Fabric. AI and machine learning understand, classify, and help develop effective responses to in-the-wild malware. Threat intelligence flows seamlessly to all Fortinet solutions and AWS integrations, often updating every few hours to ensure your environment is protected against the latest threats.

Through automated, cloud-native updates, FortiGuard Labs intelligence streams real-time threat data into AWS-deployed services. In addition, these services receive AI-driven intelligence on IP reputations, malware signatures, and web exploits directly from Fortinet's global research team to protect against known and zero-day threats, enhancing AWS workload security.

Unify your AWS security with Fortinet

In the rush to protect ever-growing attack surfaces, organizations often adopt solutions from different vendors. This can lead to fragmented security solutions that protect only part of the cloud and AI landscape. Policies contradict each other and alerts either exist in a vacuum or they generate a flood of false positives.

Fortinet removes the challenge of juggling point products. Its unified security platform empowers organizations to achieve 360-degree defense-in-depth security that protects everything from DevOps to SecOps, enabling teams to build, deploy, and run cloud applications across all environments.

Cloud security must cross multiple domains

With its unified approach, Fortinet addresses security across multiple critical domains:

Cloud network security offers comprehensive protection, visibility, and consistent policy management across AWS and hybrid environments by converging networking technologies with AI-powered security.

Web application and API protection defend against web-based threats that target known and unknown vulnerabilities.

Cloud-native application protection helps prioritize and manage risk, detect and respond to active threats, boost developer productivity, and increase security effectiveness.

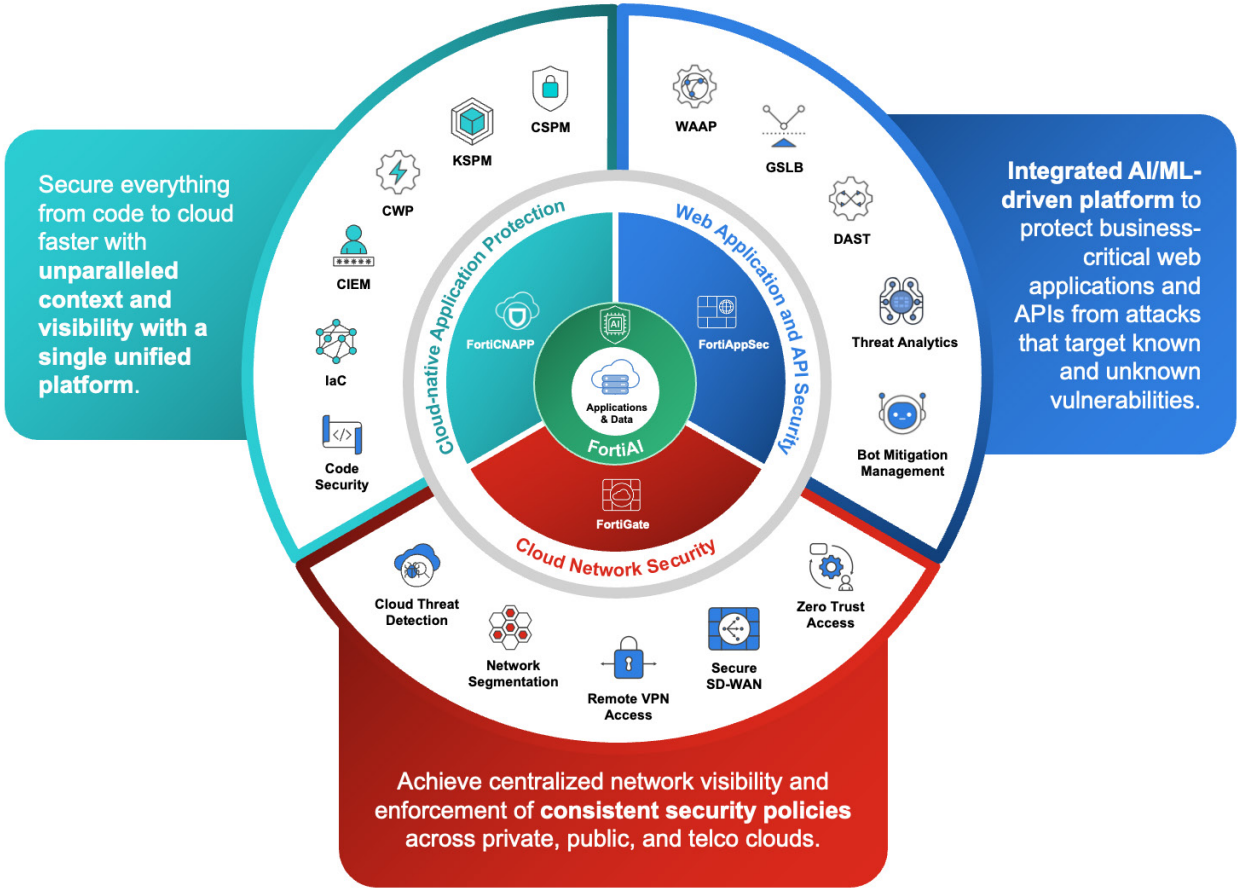
Securing your LLMs and MCP servers in runtime guards against a myriad of threats such as prompt injections, jailbreaking, excessive consumption, and data exfiltration.

> **What I like best about FortiCNAPP is its unified visibility across cloud infrastructure, workloads, and identities in a single platform. Instead of using separate tools for CSPM, CIEM, and vulnerability management, everything is integrated, which makes monitoring and remediation much more efficient. I also appreciate the real-time risk prioritization.**
>
> —Ashenafi M., Vulnerability Assessment and Penetration Tester

OPTION 1

Security that's hybrid strong

Fortinet unifies security whether you're all-in on AWS or managing hybrid environments. Its security platform provides visibility and consistent policies across clouds and on-premises infrastructure through a single management interface. By consolidating security management across clouds and on-premises deployments, Fortinet helps deliver effective and consistent security wherever your compute occurs.

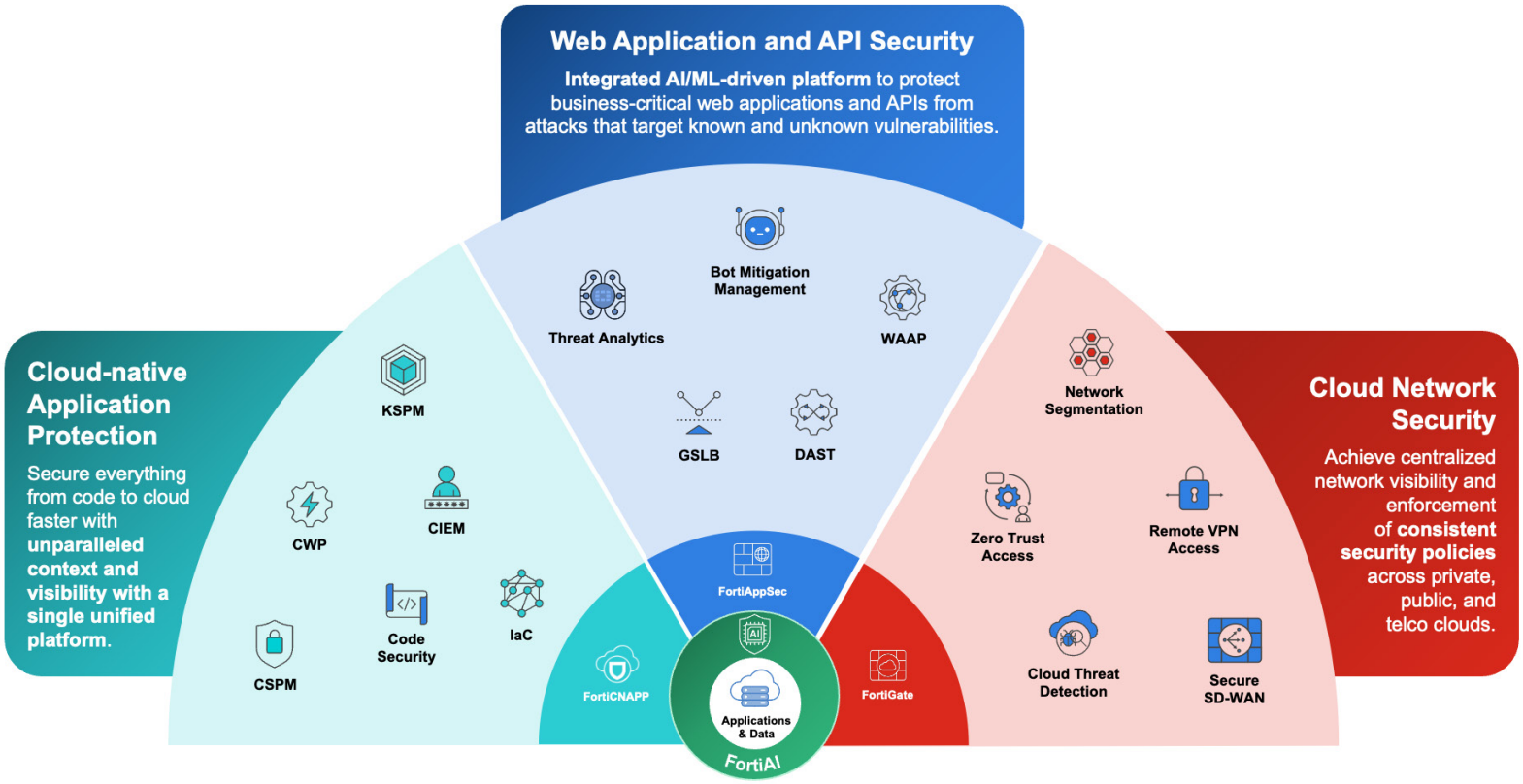


The following sections provide more detail on protecting these critical domains and the AI and agentic solutions that run through them all.

OPTION 2

Security that's hybrid strong

Fortinet unifies security whether you're all-in on AWS or managing hybrid environments. Its security platform provides visibility and consistent policies across clouds and on-premises infrastructure through a single management interface. By consolidating security management across clouds and on-premises deployments, Fortinet helps deliver effective and consistent security wherever your compute occurs.



The following sections provide more detail on protecting these critical domains and the AI and agentic solutions that run through them all.

Secure hybrid cloud networks from AWS landing zone to edge

As your organization scales across AWS regions and connects to on-premises data centers, maintaining consistent network security policies becomes increasingly difficult. However, the gaps in those policies can become attack vectors. Fortinet cloud network security solutions can help you close those gaps and deliver the consistency you need.

For organizations building on AWS Landing Zones, Fortinet adds comprehensive security and visibility across every layer of the cloud environment, ensuring a secure and compliant foundation from day one. It provides advanced network security controls that protect traffic between applications, clouds, and the internet across the multi-account environment.

Protection deployed in minutes or tailored to the edge

When your organization requires comprehensive visibility and maximum control, FortiGate VM delivers enterprise-grade next-generation firewall capabilities including secure connectivity, SD-WAN, Zero Trust Network Access, and network segmentation, all in AWS. ZTNA policies can be enforced for both remote and on-site users with granular application access controls, regardless of where users connect from or where applications reside. And integrated SD-WAN capabilities improve connectivity between branches, data centers, and AWS, reducing latency and improving application performance.

All FortiGates are powered by FortiOS, the world's most widely distributed security operating system, regardless of the form factor. This provides consistent policies no matter where the application needs to be deployed, which often reduces operational complexities in multi-cloud and hybrid-cloud deployments.

NEW!

Fortinet Managed IPS Rules for AWS Network Firewall

- You can set up enterprise-grade protection in minutes by deploying FortiGuard Labs threat intelligence directly in AWS-native services.
- Fortinet manages and continuously updates rule sets based on real-time global threat intelligence so it's always current.
- Rules include tens of thousands of signatures, delivering enterprise-grade protection that helps meet PCI DSS, HIPAA, and AWS best practices.
- Flexible AWS Marketplace pricing options.

Integration with AWS and management on your terms

FortiGate solutions work seamlessly with AWS Gateway Load Balancer, AWS Firewall Manager, and AWS Transit Gateway to simplify deployment and deliver consistent policy enforcement across your environment. And you choose the management approach that fits your operations: AWS Firewall Manager or FortiManager for centralized visibility across your entire security estate. You can also use FortiAnalyzer to centralize log management, analytics, and incident response.

Customer spotlight

BEST BUY

Challenge

Best Buy operated a complex network across MPLS, managed circuits, and cellular connectivity, which increased operational overhead and introduced application latency. This made it difficult to deliver consistent, high-performance access to cloud-based applications across store locations.

Solution

Best Buy implemented FortiGate VM NGFW with SD-WAN and AWS Transit Gateway Connect to simplify connectivity between stores and AWS.

Results

20% reduction

in latency from stores to AWS, improved uptimes, and enhanced operational efficiency.

Protect cloud applications with code-to-cloud security in a single platform

Because DevOps teams move fast, security teams can struggle to keep pace. That's how misconfigurations slip through, vulnerabilities go undetected, and compliance becomes a fire drill.

Built on AWS, FortiCNAPP is a cloud-native application protection platform (CNAPP) that provides comprehensive security from code to cloud. This platform combines Cloud Security Posture Management (CSPM), Kubernetes Security Posture Management (KSPM), Cloud Infrastructure Entitlement Management (CIEM), and workload protection (CWPP) to find, prioritize, and remediate risks across multi-cloud environments. It also operationalizes cloud infrastructure, protects workloads, secures the CI/CD pipeline, and manages risks across the entire application lifecycle.

FortiCNAPP uncovers misconfigurations and more before they hit production

FortiCNAPP shifts security left. Infrastructure-as-code scanning catches security issues before deployment, without slowing developers down. That shift matters for both sides. Developers keep their speed, and security teams aren't chasing ephemeral environments that spin up and down faster than anyone can track.

Once workloads are running, FortiCNAPP uses CSPM to monitor configurations against best practices and compliance frameworks, identifying misconfigurations before attackers do. Data Security Posture Management extends that visibility to your data itself, scanning AWS Simple Storage Service (Amazon S3) buckets to detect sensitive data exposure and malware files before they become breach headlines.

Code-to-cloud security finds threats fast and responds faster

When threats appear, FortiCNAPP finds them fast. Patented AI-powered composite alerts correlate weak signals across your environment to uncover hidden threats that point solutions miss, reducing investigation time from hours to minutes.

Containers and Kubernetes workloads get both agentless and agent-based protection for deep visibility into runtime behavior, while behavioral analytics and real-time threat intelligence detect and respond to threats targeting cloud workloads. And because FortiCNAPP integrates natively with AWS Security Hub, Amazon GuardDuty, and Amazon Inspector, it complements your existing AWS security investments rather than replacing them.

FortiCNAPP also integrates with FortiGate VM to detect its deployments along internet-accessible paths to cloud workloads, providing a comprehensive, network-aware view of exposure and security posture within your cloud environment.

Customer spotlight

coveo™

Challenge

AI-powered search company Coveo had limited visibility into a large AWS environment that was at risk through misconfigurations and compliance gaps.

Solution

FortiCNAPP provided Coveo with agentless deployment for rapid implementation, unified visibility, and posture management.

Results

Coveo achieved faster, more secure deployment without production disruption, improved compliance reporting, and reduced noise and alert fatigue for SOC analysts. Most importantly, Coveo reduced operational risk by actively identifying misconfigured assets, such as unintentionally exposed instances, and coding errors that might have exposed critical data.

FPO

Window screen placement

Defend your web applications and APIs

Web applications and APIs are your business's front door, and attackers know it. From credential stuffing to zero-day exploits to API abuse, attacks are now created by generative AI, requiring your web application firewall (WAF) to up its game to keep up with the volume or sophistication of what's coming through.

Block threats without blocking business

What sets Fortinet apart is how it handles the gray areas of cloud security. Dual-layer machine learning first evaluates traffic against known threats. Then it models your application's normal behavior to catch anomalies that signature-based tools miss, such as gen AI-created zero-days, while nearly eliminating false positives.

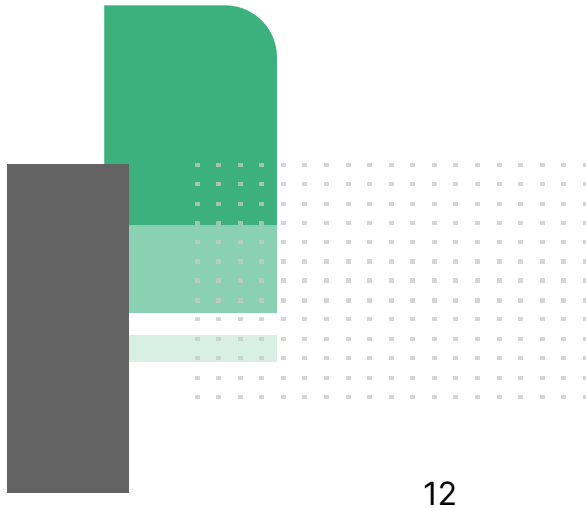
Intelligent bot detection adapts to evolving tactics, blocking credential stuffing, content scraping, data harvesting, and transaction fraud without adding friction for legitimate users. Also, dedicated API security controls protect the integrations powering your B2B workflows and mobile applications, with machine learning-based API discovery that automatically profiles your API inventory.

Whether applications are on AWS or on-premises, Fortinet delivers consistent protection and unified management across your entire web application estate.

Deploy web app and API protection that fits your environment

FortiAppSec Cloud is a SaaS-delivered solution that consolidates protections across hybrid and multi-cloud environments. It deploys in minutes with built-in setup wizards and predefined policies, and no complex configuration is needed. FortiAppSec simplifies application security and delivery across hybrid and multi-cloud environments, uniting WAF, API security, advanced bot protection, DDoS mitigation, and application performance optimization into a single, AI-driven interface.

For organizations that need more control or want to keep security closer to their workloads, FortiWeb VM delivers the enterprise-grade protection of FortiWeb, including MCP protection. This virtual appliance can be deployed directly on AWS or across hybrid environments. And for teams already invested in AWS WAF, Fortinet Managed WAF Rules bring FortiGuard Labs threat intelligence directly into your existing setup and continuously update it.



Deploy web app and API protection that fits your environment

FortiAppSec Cloud is a SaaS-delivered solution that consolidates protections across hybrid and multi-cloud environments. It deploys in minutes with built-in setup wizards and predefined policies, and no complex configuration is needed. FortiAppSec simplifies application security and delivery across hybrid and multi-cloud environments, uniting WAF, API security, advanced bot protection, DDoS mitigation, and application performance optimization into a single, AI-driven interface.

For organizations that need more control or want to keep security closer to their workloads, FortiWeb VM delivers the enterprise-grade protection of FortiWeb, including MCP protection. This virtual appliance can be deployed directly on AWS or across hybrid environments. And for teams already invested in AWS WAF, Fortinet Managed WAF Rules bring FortiGuard Labs threat intelligence directly into your existing setup and continuously updates it.

"I use FortiAppSec Cloud to secure and monitor our web applications and APIs. It helps us detect vulnerabilities, manage security policies, and maintain visibility into potential threats in our cloud environment. FortiAppSec Cloud centralizes monitoring, improves alerting, and helps us respond to risks more efficiently. One of the best features is its centralized board and control center, which offers a consolidated view of application health, threat activity, and policy status in one place.

—Manav S.,
Triage Analyst

"Fortinet adds a layer of protection for all of our applications and stores, giving them high availability and security across both cloud and on-premises environments.

—César Lino Barbato,
Infrastructure, Services and Support Coordinator, Coop

Protect LLMs, AI applications, and workloads with secure guardrails

Everyone's deploying AI; however, few companies know how to secure it. The challenges include an AI security skills gap, ML training and inference in the application layer, and blind spots caused by data flows that blend classic and AI layers.

FortiAIGate addresses the new security, governance, and operational challenges that arise when organizations deploy AI models and agents. The solution was built to ensure that sensitive data isn't leaked and that model outputs are still compliant and safe. Plus, it standardizes the connection of applications, APIs, and AI models, regardless of the provider or deployment location, without affecting the speed of innovation.

Guardrails don't have to slow innovation

FortiAIGate is purpose-built for this moment. Deployed between your applications and LLMs, it manages traffic flows and applies guardrails to every model interaction while developers keep working at their normal pace.

On the threat protection side, FortiAIGate detects and blocks prompt injection, jailbreaking attempts, model poisoning, and data exfiltration with customized guardrails for each LLM endpoint. Context-aware data loss prevention monitors both inbound and outbound AI traffic, catching sensitive data leaks and model extraction attempts before they become incidents. And the solution maps directly to OWASP Top 10 risks for LLM applications, so your coverage is comprehensive from day one.

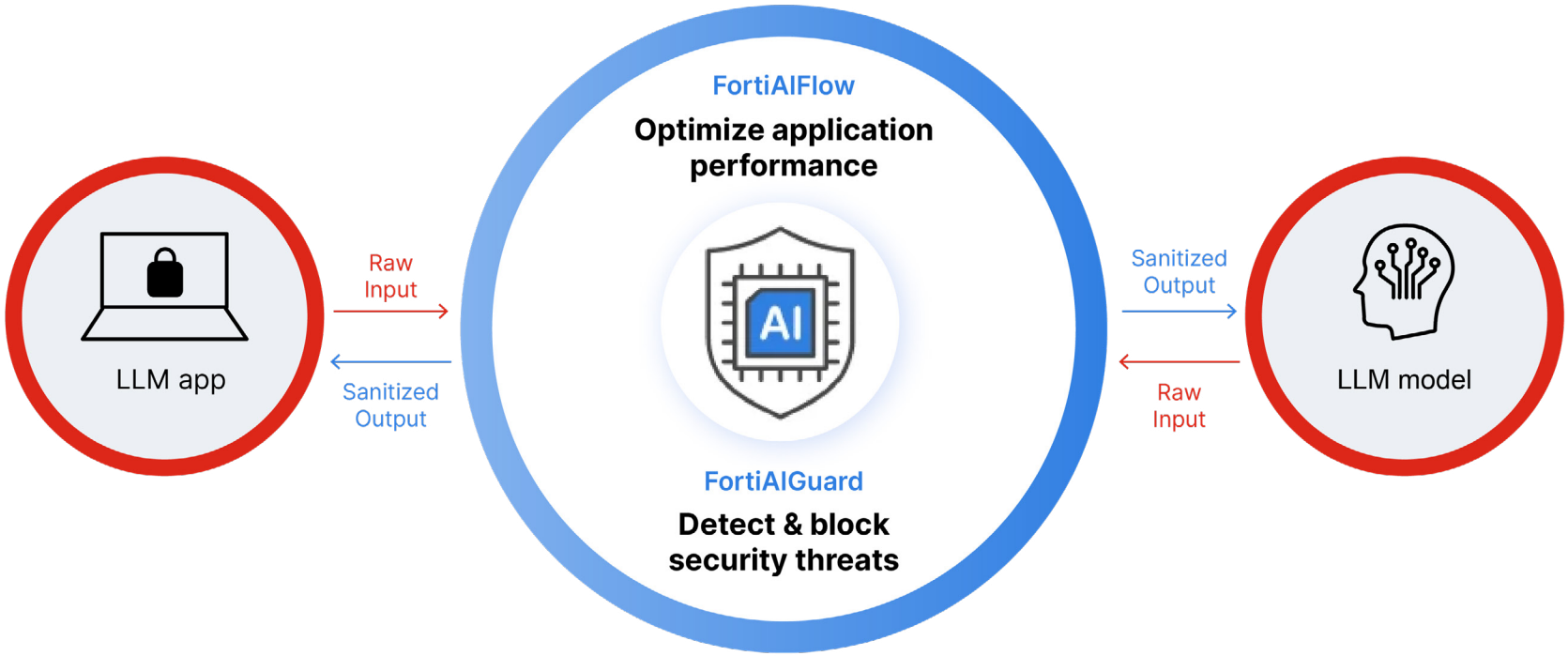
Visibility and control are over all AI environments

FortiAIGate also solves the visibility problem most organizations don't realize they have until it's too late. Centralized monitoring, auditing, and access control tell you who is using which models, with what data, under what policies across AI environments.

Built-in GUI management eliminates manual YAML configuration, while the containerized Kubernetes deployment auto-scales with LLM use. Output caching offloads duplicate tasks from models, thereby reducing token consumption and compute costs while improving response times.

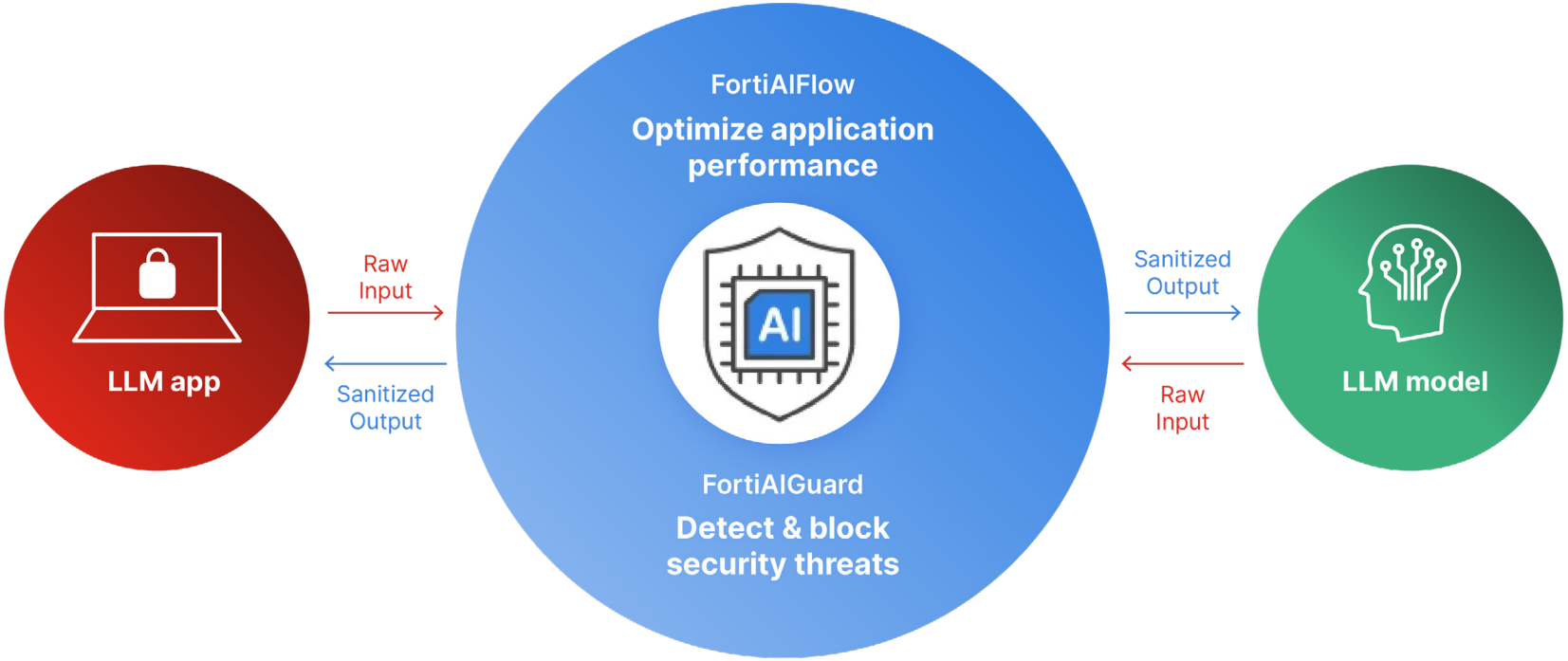
AI adoption is fast and free of unmanaged risk

FortiAIGate is also built to make AI adoption faster and more cost-efficient. Intelligent routing directs AI queries to the optimal model based on cost, latency, and performance, so teams can scale AI experimentation without introducing unmanaged risk. Meanwhile, traffic steering, caching, and workload optimization reduce unnecessary API calls and keep model usage costs predictable. The result is a foundation where security and performance reinforce each other.



AI adoption is fast and free of unmanaged risk

FortiAIGate is also built to make AI adoption faster and more cost-efficient. Intelligent routing directs AI queries to the optimal model based on cost, latency, and performance, so teams can scale AI experimentation without introducing unmanaged risk. Meanwhile, traffic steering, caching, and workload optimization reduce unnecessary API calls and keep model usage costs predictable. The result is a foundation where security and performance reinforce each other.



Accelerate your AWS security journey with expert guidance

You know where you want to go, but getting there is fraught with challenges. The rapidly evolving threat landscape, competing priorities, and a security skills shortage can overwhelm even well-resourced teams tasked with designing and implementing cloud security. Fortinet Cloud Consulting Services can help you address these challenges and more.

Design a security architecture built for your environment

Fortinet's consulting team can evaluate your current security posture, then align findings to your business goals, strategy, and compliance requirements. The result is a cloud security architecture designed around best practices and customized for your AWS and hybrid environments—not a cookie-cutter template.

Engagements can include:

- Cloud security assessments of your existing AWS deployments
- Secure migration and implementation for workloads moving to AWS
- Best-practice architecture recommendations that scale globally
- Automation for zero-touch provisioning using AWS CloudFormation or HashiCorp Terraform

Fortinet's team can also deliver customized workshops to upskill your organization, from hands-on practitioners to executive stakeholders.

Respond faster when incidents occur

When something goes wrong, speed matters. Fortinet's AWS Incident Response practice provides rapid access to security experts. These experts can help you contain threats, investigate root causes, and recover operations. Whether you're dealing with an active breach or want to be ready to respond, Fortinet's team brings decades of experience and a direct connection to FortiGuard Labs threat intelligence. The goal is to fix what's broken and then take steps to strengthen your security posture so you're more resilient the next time.

Take the next step

Fortinet enables organizations to secure their AWS networks, applications, and AI workloads with a unified, AWS-native security platform that reduces complexity, delivers consistent protection, and scales as cloud environments evolve. And because it's a platform, it provides consistent policies, centralized visibility, and AI-powered intelligence.

From landing zone to LLM, Fortinet has you covered.

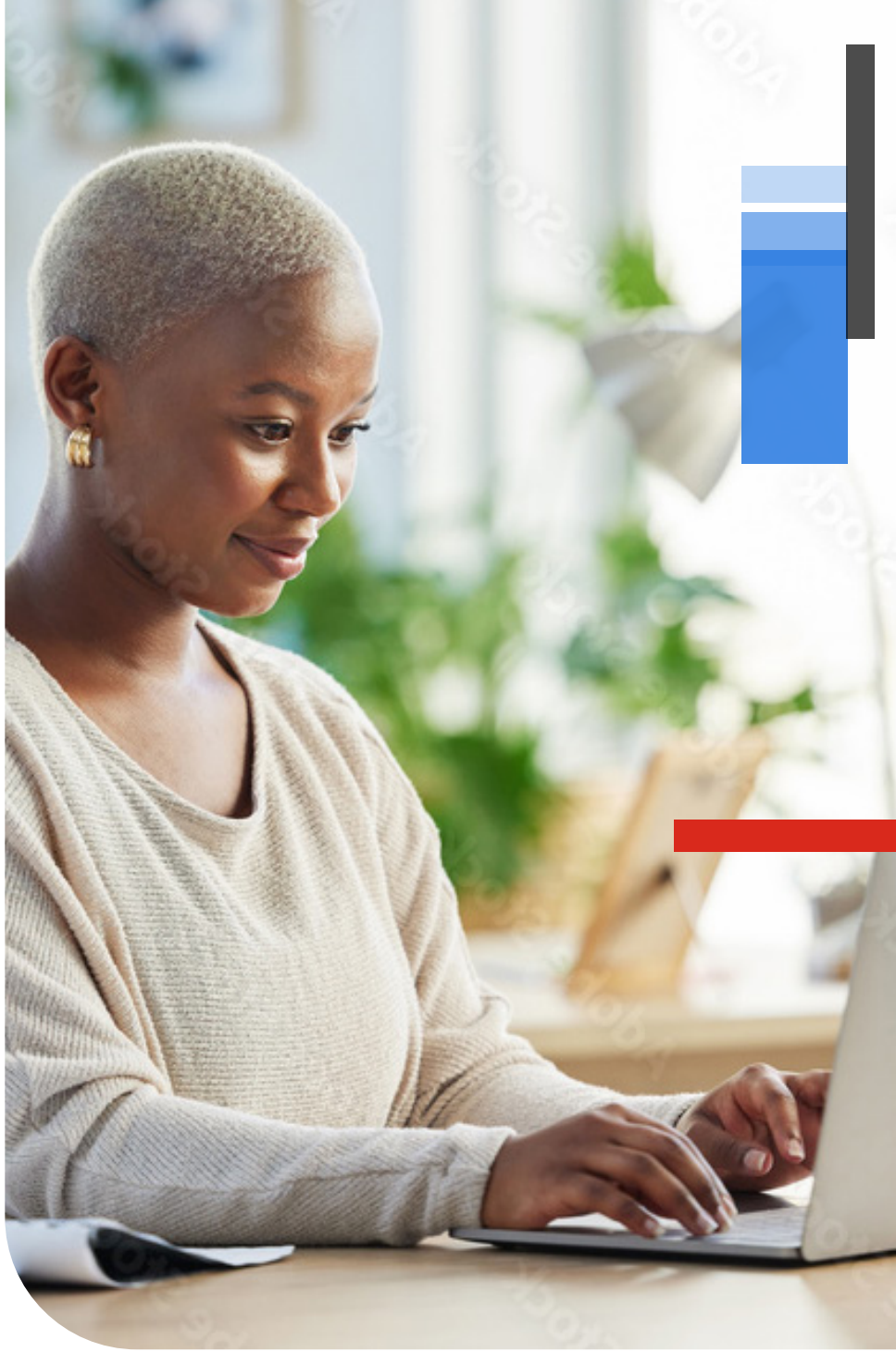
Get started with flexible deployment and licensing in AWS Marketplace

Fortinet solutions are available in AWS Marketplace. There are options for every deployment model and budget, either pay as you go or annual contracts. In addition, the FortiFlex program from Fortinet delivers flexible, simple on-demand licensing and provisioning for security solutions and services for all environments.

Browse Fortinet solutions in AWS Marketplace

Learn more

EXPLORE FORTINET SOLUTIONS FOR AWS



April 2026