aws | **F⊟RTINET**®

Protecting the Health of the Healthcare Ecosystem on AWS

Secure healthcare starts with protecting 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?

Overview			Use Cases						Why AWS and Fortinet	
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	Healthcare Use Cases	Cloud Consulting	AWS Marketplace

Cloud Security Transformation Strategy: Priorities-to-Gaps-to-Benefits

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

The Challenges of Protecting Data-Rich Health Ecosystems

IT teams often inherit legacy applications and devices as other organizations are acquired. It's essential to protect these systems and the connections to those systems. But this is difficult in an industry where spending on InfoSec can sometimes be less than other industries.

Securing Cloud Services and Apps

Not all systems reside in an on-premises data center—many applications and services run on the public cloud and across hybrid cloud environments. With cloud infrastructure and cloud-enabled apps arises DevOps and DevSecOps. It's vital to connect cloud and application operations, remembering that cybersecurity is a team sport; break down the functional silos.
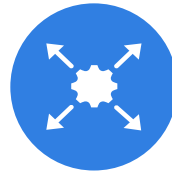
Connected Health Ecosystem

IoT makes it is easy to add new services and capabilities to the patient care portfolio, but it's also more challenging to handle the scale. Additionally, many of these devices require remote access for use, maintenance, and upgrades. Any weakness here can prove challenging and expensive to clean up security gaps after a compromise.

Resiliency and Response

A Managed Security Service Provider (MSSP) can provide core security management components such as vulnerability management services and incident response playbooks. An MSSP can also take the operations to the next level by delivering playbook automation and response orchestration. As one example, response to a phishing attack should be automated for most organizations.

Skills and Staffing Gaps

With millions of open IT security positions across all industries, staying secure and competitive with wages is a significant challenge for the healthcare industry. To take on this challenge, consider hiring individuals to fit with your culture over their experience, as you can always train for the necessary skills. You can also leverage partner services to help keep augment the resources required.

Overview			Use Cases						Why AWS and Fortinet	
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	Healthcare Use Cases	Cloud Consulting	AWS Marketplace

The Need for End-to-End Visibility and Control

The healthcare industry faces several IT challenges, from cyberattacks to increasingly complex cloud environments. Healthcare organizations are finding it difficult to keep their operations secure and patient safety intact due to:

Rising Ransomware

US cyber insurance loss ratio remains elevated in 2021, with ransomware accounting for three-quarters of claims.[1]

Growth of IoMT

The number of Internet of Medical Things (IoMT) devices is expected to exceed 7M by 2026, with nearly 4K devices per hospital.[2]

Record Mergers & Acquisitions

13 transactions generated $19.2B in activity in Q2 2022, a new record.[3] The resulting disruption increases risk.

1. The Geneva Association, Ransomware: An insurance market perspective, July 2022
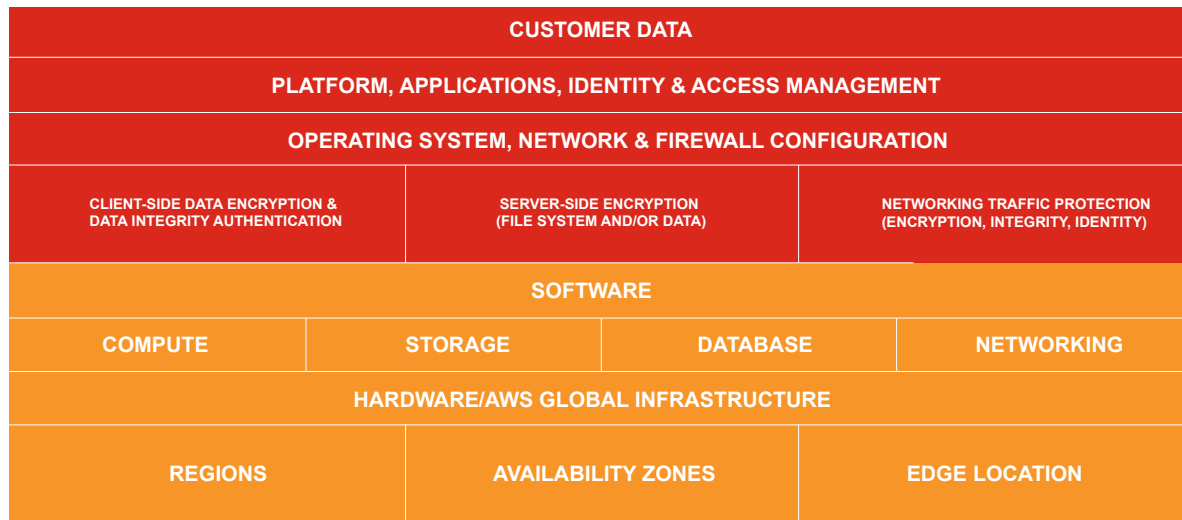2. Juniper Research, Smart Hospitals: Using Big Data to Enhance Healthcare Delivery, January 2022
3. Kaufman Hall, M&A Quarterly Activity Report: Q2 2022, July 2022

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.

Security IN the Cloud

FORTINET®

CUSTOMER DATA			
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT			
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION			
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)		NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
SOFTWARE			
COMPUTE	STORAGE	DATABASE	NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE			
REGIONS	AVAILABILITY ZONES		EDGE LOCATION

Security OF the Cloud

aws

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.

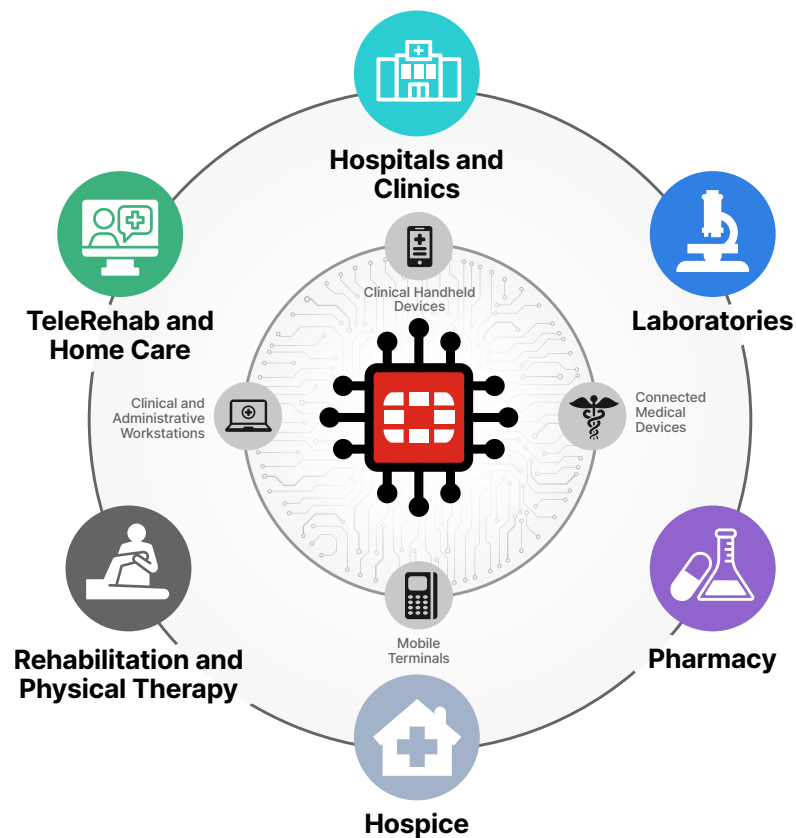| Overview			Use Cases						Why AWS and Fortinet	
Intro	Security Fabric	End-to-end Visibility	Hybrid-Cloud Security	Cloud-Native Network Security	Web Application & API Protection	Risk Management & Visibility	Zero Trust Network Access	Healthcare Use Cases	Cloud Consulting	AWS Marketplace

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
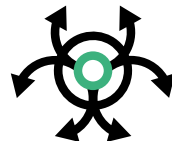
18 million network intrusion attempts resisted per minute
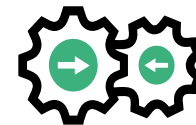
1 billion security updates produced every day

FortiGuard Labs
Global threat research and response

End-to-End Visibility and Control for Patient Care and Employee Experience

Fortinet offers a complete ecosystem of security products that complement our Secure SD-WAN and NGFW solutions and meet the needs of the smallest doctor's office to the largest health insurer's data center. Our solutions span today's most data-intensive industries, including government, healthcare, financial services, and education. And as these fields continue to evolve at a feverish pace, companies are increasingly looking to Fortinet as an experienced, leading-edge security partner.

Hospitals and Clinics

TeleRehab and Home Care

Laboratories

Clinical Handheld Devices

Clinical and Administrative Workstations

Connected Medical Devices

Rehabilitation and Physical Therapy

Mobile Terminals

Pharmacy

Hospice

32X
Faster Encryption

300%
SD-WAN ROI

88%
Lower Power Consumption

17X [*]
Security Compute Rating

7 of 10
Top Ten Healthcare
use Fortinet

7 of 10
Top Ten Big Pharma companies
use Fortinet

Fortinet Achieves 99.88%
Security Effectiveness Score
on industry's only independent next-generation firewall test [Read the press release]

*Source: Fortinet Unveils New ASIC to Accelerate the Convergence of Networking and Security Across Every Network Edge.

Overview			Use Cases						Why AWS and Fortinet	
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	Healthcare Use Cases	Cloud Consulting	AWS Marketplace

End-to-End Visibility and Control Across Healthcare 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 post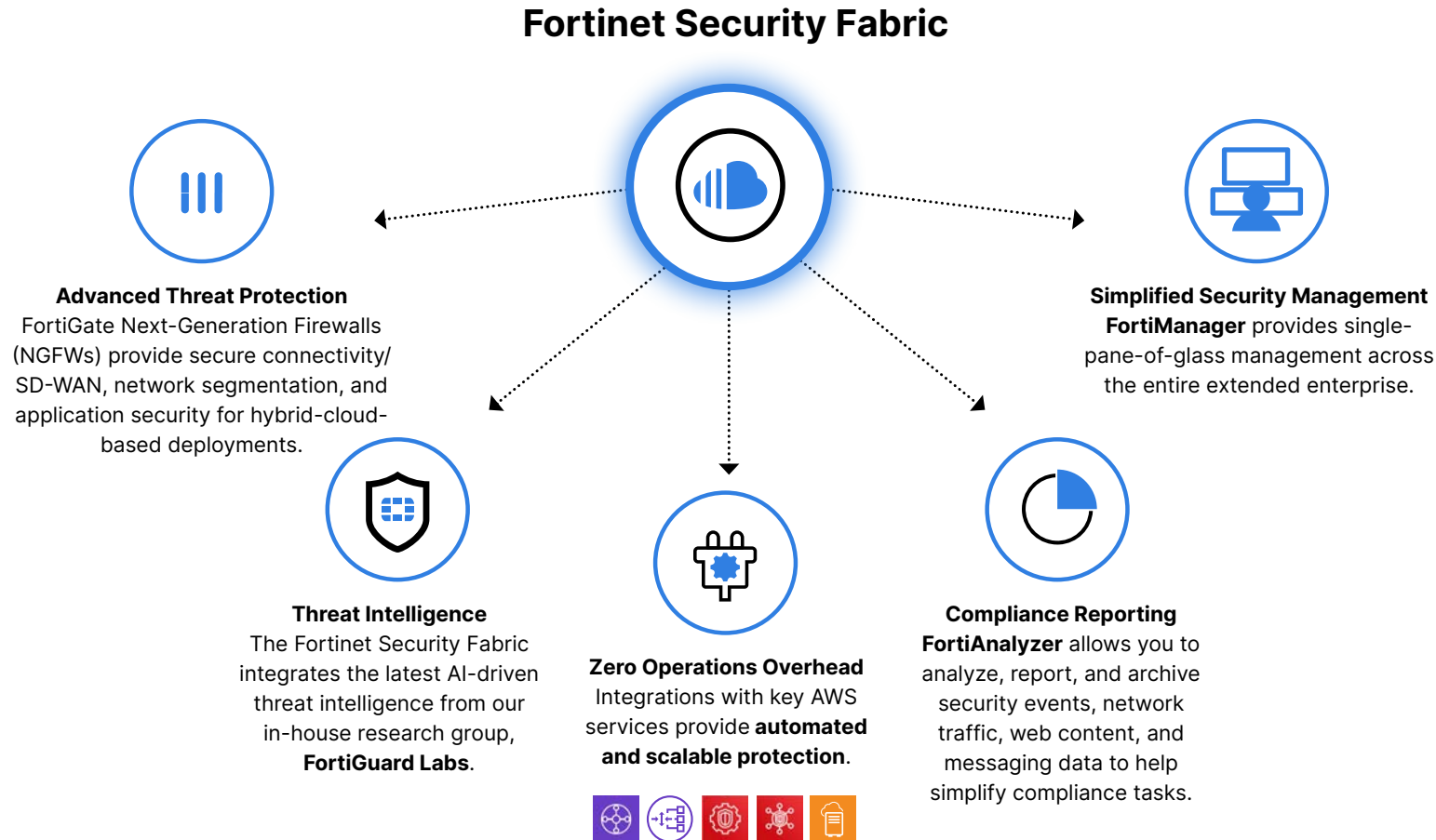ure for hybrid-cloud use cases through natively-integrated security functionality that works across AWS services such as Amazon GuardDuty, AWS Security Hub, and AWS Firewall Manager. The integrated single-plane-of-glass management helps you streamline operations, ensure policy consistency, and unify 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.

Use Cases	Hybrid-Cloud Security, Natively Delivered		Web Application and API Protection		Risk Management and Visibility			Zero Trust Network Access	
Benefits	Centralized visibility, control, and automation simplified		Protect against OWASP Top 10 threats, zero-day, and other app layer attacks		Manage cloud risks with actionable insights			Enforce ZTNA policies for both remote workers and on-campus workers	
Fortinet Solutions	FortiGate Cloud-Native Firewall (CNF)	FortiGate-VM	FortiWeb Cloud WAF-as-a-Service	Fortinet Managed Rules		FortiCNP Cloud Native Protection		Fortinet Zero Trust Access	+ Fortinet ZTNA Application Gateway
AWS Integrations	AWS Firewall Manager	Gateway Load Balancer	AWS WAF		AWS Security Hub	Amazon GuardDuty	Amazon Inspector	AWS Firewall Manager	AWS Gateway Load Balancer

Overview		Use Cases						Why AWS and Fortinet	
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	Healthcare Use Cases	Cloud Consulting	AWS Marketplace

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

Retain consistent protection and visibility across distributed healthcare 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.

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

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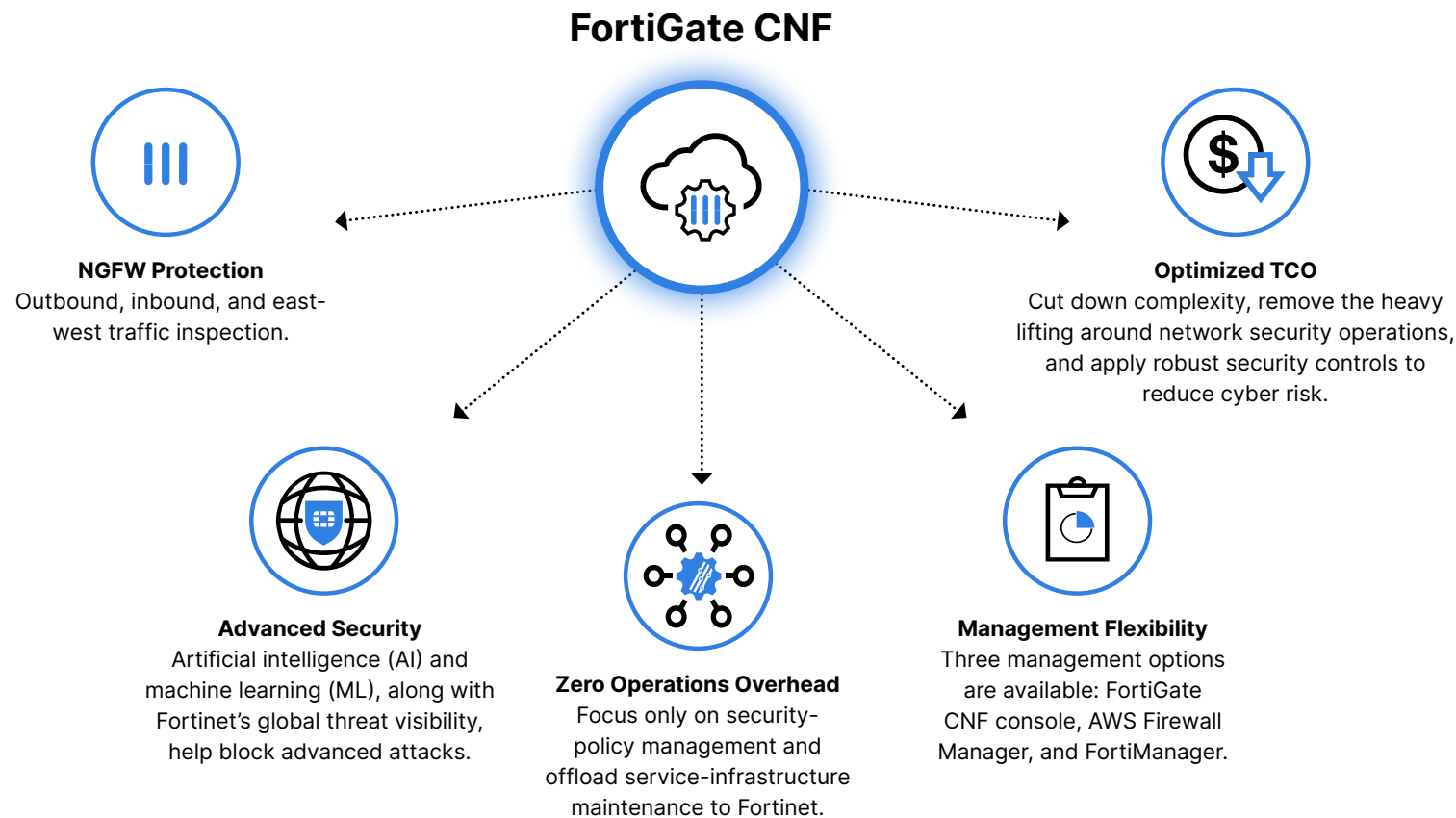
Hybrid cloud deployments that unite on-premises data centers and workloads on AWS provide much-needed flexibility for healthcare organizations to modernize and innovate across environments. But security across these extended environments tends to be inconsistently enforced and complex to manage.

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

Overview	Use Cases						Why AWS and Fortinet	
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	Healthcare Use Cases	Cloud Consulting	AWS Marketplace

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.

Optimized TCO
Cut down complexity, remove the heavy lifting around network security operations, and apply robust security controls to reduce cyber risk.

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.

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.

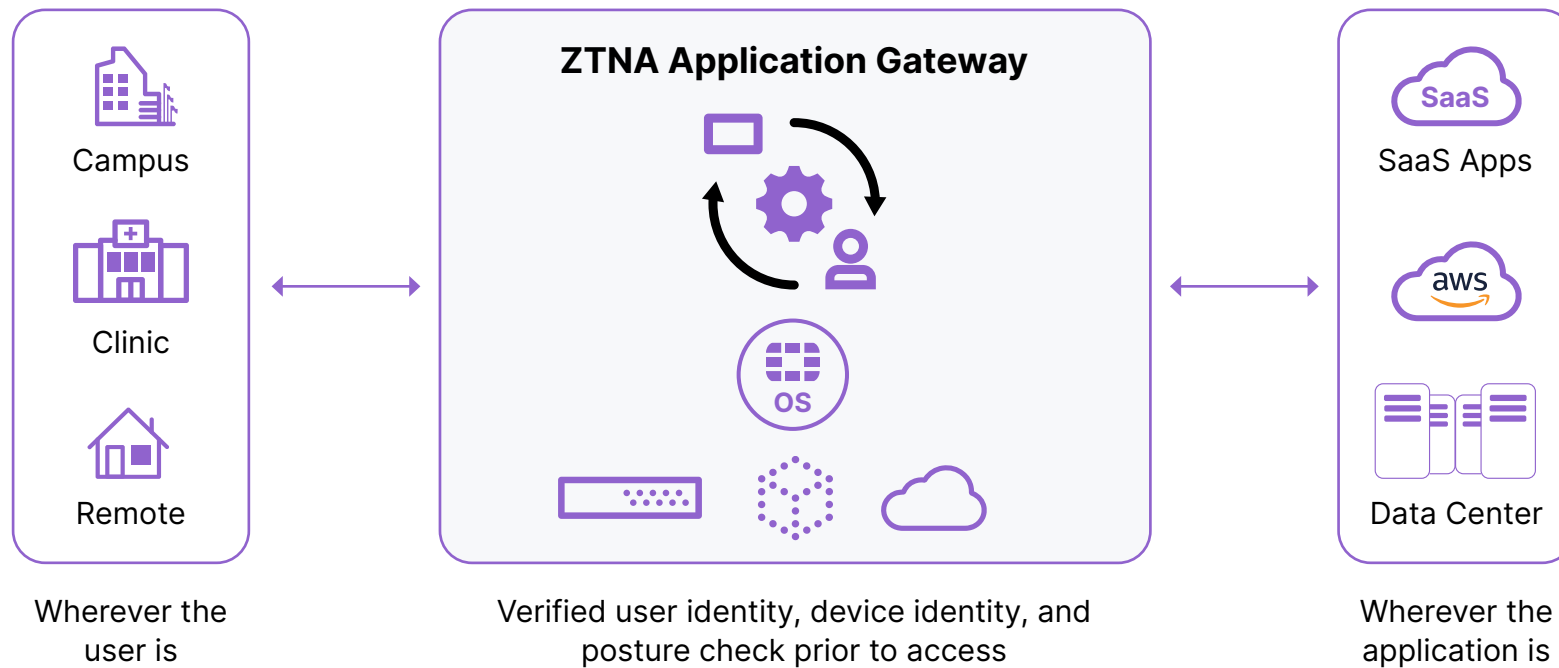| Overview			Use Cases					Why AWS and Fortinet	
Intro	Security Fabric	End-to-end Visibility	Hybrid-Cloud Security	Cloud-Native Network Security	Web Application & API Protection	Risk Management & Visibility	Zero Trust Network Access	Healthcare Use Cases	Cloud Consulting	AWS Marketplace

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

FortiCNP

Fortinet Cloud Security Fabric

FortiGuard Threat Intelligence

Cloud Security Posture Management	**Cloud Workload Protection**	**Vulnerability Management**	**Data Security**	**Network/Threat Detection**	**Container Protection**

AWS Security Hub Controls | **Amazon GuardDuty- Malware Protection, EKS, CloudTrail** | **Amazon Inspector** | **Amazon GuardDuty for S3** | **Amazon GuardDuty-VPC Flow Logs** |

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

Campus		ZTNA Application Gateway		SaaS Apps
Clinic				
Remote				Data Center

Wherever the user is

Verified user identity, device identity, and posture check prior to access

Wherever the application is

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.

Fortinet Helps Reduce Operational Overhead and Increase Security Efficacy

> "
> We needed to go beyond the compliance checkbox for our AWS environment. Fortinet went above and beyond to deliver a best-in-class Next Generation Firewall IPS solution that ties us back to our philosophy that cybersecurity is equivalent to patient safety.
>
> — Jason Viera, Global Network Ops Leader, Philips Healthcare Informatics

To stay ahead of the rapidly evolving threat landscape, healthcare 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 that could put patient safety at risk.

Statewide Healthcare Provider Securely Connects Remote Sites and Devices

In a widely dispersed healthcare system, technology plays a key role in providing doctors, nurses, and caregivers with secure access to information and tools. To ensure sensitive data is secure, a state-wide healthcare provider upgraded how remote facilities and medical devices connected to its data center with FortiGate Next-Generation Firewall and Fortinet Internal Segmentation Firewall.

- Improved performance and network uptime
- More time for engineers to monitor and analyze collected data
- New levels of engineer confidence in the network
- Able to segment the network to protect valuable assets

> "
> The IT team also spoke with industry analysts and a network security consultant, who reviewed our network design and validated that Fortinet would be the right choice.
>
> — CISO

Regional US Healthcare Provider with Out-of-Control IoT

A US healthcare organization supported a large number of unmanaged and potentially insecure connected medical devices on its network. To better secure its disparate devices and protect its assets, the organization deployed FortiGate Next-Generation Firewalls for micro-segmentation and FortiNAC for more granular access policies.

- Near real-time visibility into emerging threats and attacks for overall efficacy of the security environment
- Single pane-of-glass management and complete visibility of connected medical devices
- Better risk management through improved security
- Consolidated toolset that integrates seamlessly at the core

> 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

National US Nursing Provider Benefits From Network Security Convergence

A large nursing home provider operating 61 sites was suffering from a problematic SD-WAN rollout. Fortinet helped them achieve converged security and networking across sites with FortiGate Secure SD-WAN. FortiGate NGFWs plus FortiGuard Labs was deployed for real-time security services to prevent known and unknown threats from entering the network.

- 40% reduction each week in staff time spent managing networking and security infrastructure
- Improved, real-time security for sensitive data
- Strengthened compliance with federal regulations around patient care and data security

"

The Fortinet Security Fabric approach created a single, unified solution for us. We found individual products that met our specific requirements, and they integrated seamlessly.

— VP and IT Security Officer

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

Overview			Use Cases						Why AWS and Fortinet	
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	Healthcare Use Cases	Cloud Consulting	AWS Marketplace

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
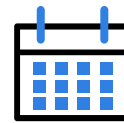
Annual and Multi-year

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

Find Your Path to Enable Healthcare Innovation with Fortinet and AWS

	EXPLORE	**EXAMINE**	**EXPERIENCE**
Business	On-Demand Webinar: Cloud-Native Security: Trends and Best Practices	ESG eBook: Looking to Modernize Network Security on Public Clouds?	Video Case Study: Philips Healthcare
Operations	Case Studies: Healthcare Sector	eBook: Security Considerations for Your AWS Cloud Migration	Find Fortinet solutions on the AWS Marketplace
Technology	PeerSpot Report: Top 6 Selection Factors for NGFW for Cloud Environments	Point of View: Secure Radiology: The Urgency To Protect Remote Radiologists	Deployment & Architecture Guides

To learn more about Fortinet and AWS, visit www.fortinet.com/aws.

To explore Fortinet and AWS solutions designed to protect the healthcare sector, visit https://www.fortinet.com/solutions/industries/healthcare.

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

aws | **FÜRTINET**®

www.fortinet.com/aws

June 09, 2023 4:00 PM

Fortinet_AWS_B2G_e

123456-0-0-EN

Overview			Use Cases						Why AWS and Fortinet	
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	Healthcare Use Cases	Cloud Consulting	AWS Marketplace