

SOLUTION BRIEF

Security That Moves at the Pace of Healthcare with Fortinet and AWS

Executive Summary

Healthcare modernization is reshaping both care delivery and the systems behind it. AI is entering clinical workflows, care is extending beyond hospital walls, health data is moving across increasingly connected environments, and patients and clinicians are depending on digital services at every step. That creates a difficult mandate for security teams: protect sensitive data and critical systems without slowing access, innovation, or care delivery.

Fortinet and Amazon Web Services (AWS) help healthcare organizations meet that challenge with integrated security across cloud, clinical, and connected care environments. Together, they help turn modernization initiatives into secure outcomes.

Healthcare Security Cannot Stop at the Cloud Boundary

Security risk is not confined to a single system or workload. It follows the paths that users, data, and traffic take across clinical systems, cloud services, applications and APIs, and connected devices. When those environments are secured separately, IT teams can lose the visibility and consistency they need to manage risk effectively.

What’s needed is a security approach that keeps safeguards close to the systems and data they protect, gives IT teams the visibility to understand when activity could affect care, and supports faster response when action is required. Fortinet and AWS solutions help IT teams meet today’s priorities and protect what’s next.



“Riverside’s doctors and colleagues are continually impressed with our ability to quickly address the latest security challenges using Fortinet.”

Erik Devine, Chief Security Officer, Riverside Healthcare

Case Studies	
Bring AI into care with control built in Adopt AI while keeping prompts, patient context, and AI-generated guidance within governed workflows.	- FortiAI Gate provides a security gateway between AI applications and AWS AI services such as Amazon Bedrock and Amazon SageMaker, protecting prompts, models, and sensitive clinical data while helping defend against prompt injection, data leakage, and other emerging AI threats. - Fortinet cloud-native application protection (FortiCNAPP) and Fortinet DLP help protect AWS workloads and the sensitive data that AI workflows rely on.
Extend care beyond the hospital Give clinicians secure access to the resources they need while protecting clinical systems and PHI from unnecessary exposure.	- FortiSASE and FortiGate enforce ZTNA policies and device posture checks before granting remote clinicians access to approved applications and virtual care resources. - FortiSASE can also extend secure access to remote IoT and IoMT devices, including those that cannot run an endpoint client.
Protect the medical records care depends on Protect clinical data as EHR workloads extend beyond the data center.	- FortiGate VM integrates with AWS networking services to inspect and segment EHR-connected traffic across cloud and hybrid environments, helping protect PHI as it moves between clinical systems and traffic paths. - FortiAnalyzer and FortiManager centralize logging, visibility, and policy management across Fortinet-protected environments, helping IT teams apply security controls more consistently across connected systems and traffic paths.

See risk in context and act faster

Give security teams the visibility to recognize and contain threats before they disrupt care.

- FortiSIEM brings security activity from Fortinet-protected environments, AWS-connected workloads, and care-supporting systems into a shared investigation view, helping analysts understand what happened, what may be affected, and where response should begin.
- FortiNAC extends visibility to connected devices by discovering and profiling IoT and IoMT equipment, feeding real-time risk telemetry into FortiSIEM and AWS Security Hub, and enabling isolation when containment is required.

Keep care-critical apps and APIs available

Protect the digital services patients and clinicians depend on from attacks, abuse, and disruption.

- FortiWeb VM and FortiAppSec Cloud work alongside Amazon API Gateway to protect healthcare applications and APIs from OWASP vulnerabilities and threats affecting SMART on FHIR data flows.
- Bot mitigation distinguishes legitimate human traffic from malicious automation to stop credential abuse, scraping, fraud, and other activity that can interfere with application access and use.

Integrated Security for Connected Healthcare

Fortinet integrates with AWS networking and security services to extend protection and visibility across AWS, clinical environments, applications, users, and connected systems.

Together, Fortinet and AWS help healthcare organizations:

- Protect consistently across AWS, on-premises, and distributed care environments
- Simplify operations with integrated visibility, policy, and automation
- Innovate securely as cloud, digital care, and AI initiatives expand

Keep Healthcare Innovation Moving Securely

Healthcare priorities will continue to evolve. Fortinet and AWS give security teams the flexibility to address today's requirements while extending protection as cloud, clinical, and AI environments change.

Ready to strengthen security where it matters most? [Explore Fortinet solutions for AWS.](#)



www.fortinet.com