SOLUTION OVERVIEW

Improve Epic Application Security, Uptime, and Performance with F5 and AWS

Seconds count when it comes to accessing electronic medical records. F5 and AWS solutions ensure Epic applications are fast, secure, and available for charting, orders, patient records, scheduling, billing, and more.

aws PARTNER

KEY BENEFITS

Improve security posture
Protect your Epic applications from threats with consistent policies, advanced defenses, and automation.

Increase uptime and reliability
Eliminate the main causes of outages to keep patient care on schedule and improve outcomes.

Ensure regulatory compliance
Demonstrate compliance with security and privacy regulations from governments and industry regulators.

Boost performance
Deliver faster applications and a better user experience with real-time traffic optimization and on-demand cloud resources.

Reduce costs
Leverage templatized deployments, cloud elasticity, and automation to use fewer resources.

Centralized Management and Monitoring
F5 provides centralized management and monitoring capabilities, allowing for efficient management of application delivery policies, configurations, and monitoring of application performance. This centralized approach helps in simplifying operations in an AWS environment.

Simplify operations
Monitor and manage application delivery policies, configurations, and performance in your AWS environment.

NOTABLE CYBERATTACKS IN 2021 AND 2022 COST EACH IMPACTED HEALTHCARE ORGANIZATION OVER $100M.[6]

Cyberattacks and Outages Threaten Healthcare Operations

The number of healthcare data breaches has doubled in the past three years,[1] with over 51 million healthcare records exposed in 2022.[2] These breaches average over $10 million each in cleanup costs, regulatory fines, and lawsuits.[3]

In addition, electronic medical record (EMR) outages caused by security incidents or network issues impact patient care. A study of ransomware attacks on U.S. hospitals found that they caused delays in patient care, procedure and appointment cancellations, and ambulance diversion.[4] Even data breach remediation processes were shown to have a negative impact on patient outcomes.[5]

Many IT and security teams are understaffed, which can lead to unpatched vulnerabilities, slow remediation times for security incidents, or errors from trying to work quickly. In addition, the complex configurations required for Epic's many applications, whether hosted on-premises, on AWS, or via Epic SaaS, can result in misconfigurations that impact application security or reliability.

Protect Data and Operations with F5 and AWS

Keep your Epic applications fast and available with F5 BIG-IP, no matter where they are deployed.

Block security threats that can lead to breaches or outages

Reduce misconfigurations that can impact performance

Increase availability and scalability for improved uptime

Secure Epic Application Data and Access

F5® BIG-IP® Advanced WAF® on AWS protects Epic applications from security threats that can lead to a breach of protected health information or service outage. Pre-built, validated policies for Epic can be customized to meet each organization's needs. They can also be combined with F5 Application Services Templates (FAST) to automate the configuration of BIG-IP Advanced WAF in your AWS environment. With the ability to quickly and easily customize configurations, administrators can take advantage of best practices and rapidly deploy new Epic applications with less effort.

KEY FEATURES

Pre-built policies and templates
Follow best practices with validated policies and templates designed for Epic applications.

Behavioral DDoS protection
Identify layer 7 attacks in real time to block malicious traffic.

Compliance dashboard
See the level of mitigation against the OWASP Top 10 to better understand and report security posture.

Traffic management
Steer traffic to the best available server to increase performance.

Right-size infrastructure
Resize infrastructure quickly to meet growing needs in minutes.

Granular customization
Create security policies or traffic management rules to meet specific needs.

Centralized management makes it easier to maintain consistent policies across the entire environment, inheriting security and compliance controls in AWS and creating a better security posture. Machine learning, behavioral analysis, and security intelligence identify and block sophisticated threats while allowing access to legitimate users.

Advanced WAF protects against:

- The OWASP Top 10
- Bad bots that scrape data or create fake accounts
- DDoS attacks that can slowdown apps or take them offline
- Credential stuffing attacks that can lead to a data breach
- API attacks on your third-party integrations with Epic

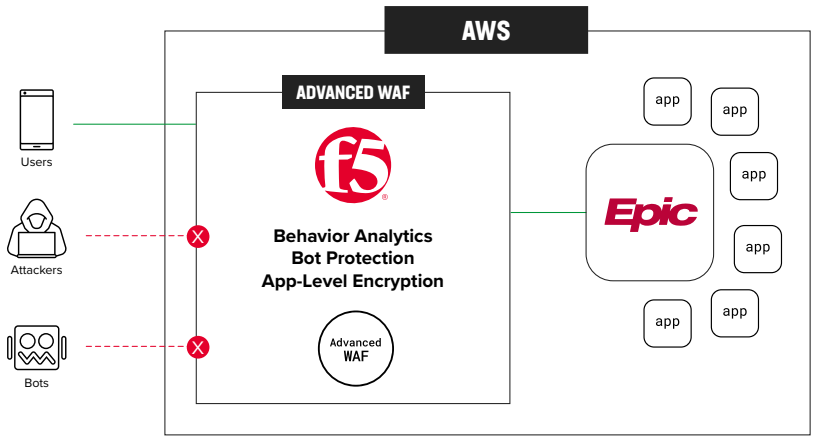

Figure 1: F5 BIG-IP Advanced WAF makes protection easier.

Reduce Misconfigurations and Errors

Deploying a new Epic application can be complicated, and a misconfiguration could result in poor performance or a security risk. Manual, one-off deployments are also time consuming and can result in configuration drift.

F5 can help deploy Epic applications in just minutes with pre-built templates that follow best practices and industry standards. These FAST templates for BIG-IP are regularly updated to ensure the best performance. They require minimal variables to reduce the risk of error and provide consistent configurations no matter where apps are deployed.

Use FAST templates with HashiCorp Terraform or Red Hat Ansible automation for even faster and more accurate deployments in multiple AWS instances or data centers.

Increase Availability and Scalability

When Epic applications run slowly or are unavailable, they create extra work and frustration for medical staff and patients. Delays in accessing records or relying on paper backups can impact quality of care.

F5® BIG-IP® Local Traffic Manager™ (LTM) and F5 BIG-IP DNS can scale and optimize network traffic so Epic applications remain fast and accessible in your AWS or hybrid environment. Monitor service health to steer traffic to the best available server or automatically failover to a backup location. Use network isolation to separate application web front ends from back-end databases for greater protection. Adjust authorization levels to applications based on the user and location to maintain compliance.

BIG-IP can be deployed both on-premises with hardware and or on AWS or other clouds with virtual editions. It can scale applications on demand to improve load times and user experience. Built-in DNS security blocks malicious communications that could slow performance or increase infrastructure costs, and SSL offloading helps increase server performance by having BIG-IP manage encryption and decryption.

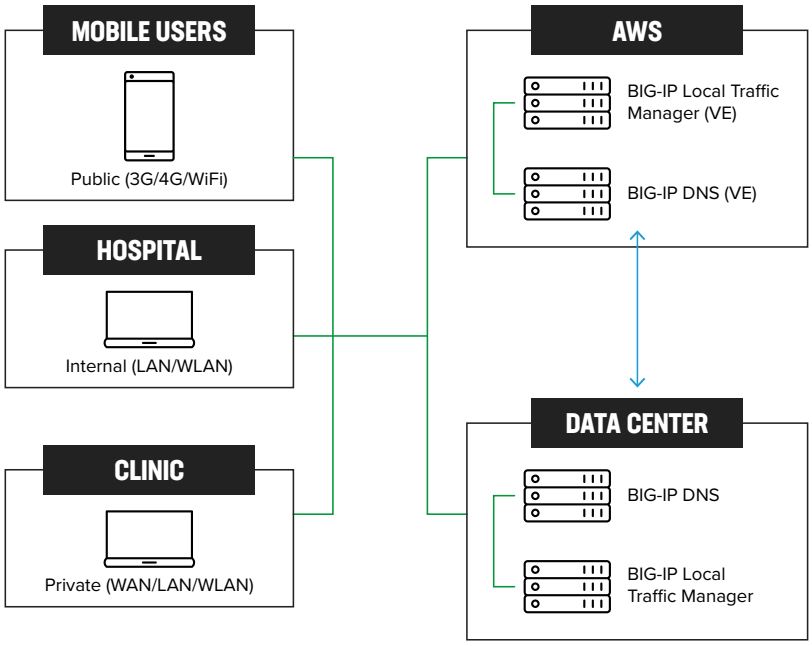

Figure 2: Increase availability and performance with BIG-IP local and global traffic management.

Protect Epic Healthcare Data and Operations with F5 and AWS

Combining BIG-IP Advanced WAF, BIG-IP LTM, and BIG-IP DNS on AWS with Epic applications keeps healthcare data and operations secure and reliable. Improve security posture and quality of care while increasing IT and medical staff efficiency with Epic applications that are always fast and available.

Learn more about F5 security and performance solutions for Epic at f5.com/epic.

[1] U.S. Dept of Health and Human Services, 2022 Healthcare Cybersecurity Year in Review, Feb 2023
[2] HIPAA Journal, 2022 Healthcare Data Breach Report, Jan 2023
[3] IBM, Cost of a Data Breach Report, July 2022
[4] Neprash HT, et al, Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021, JAMA Health Forum, Dec 2022
[5] Choi SJ, et al, Data breach remediation efforts and their implications for hospital quality, Health Serv Res, Oct 2019
[6] SC Media, CommonSpirit Health cyberattack, month-long network outage cost $150M, Feb 2023