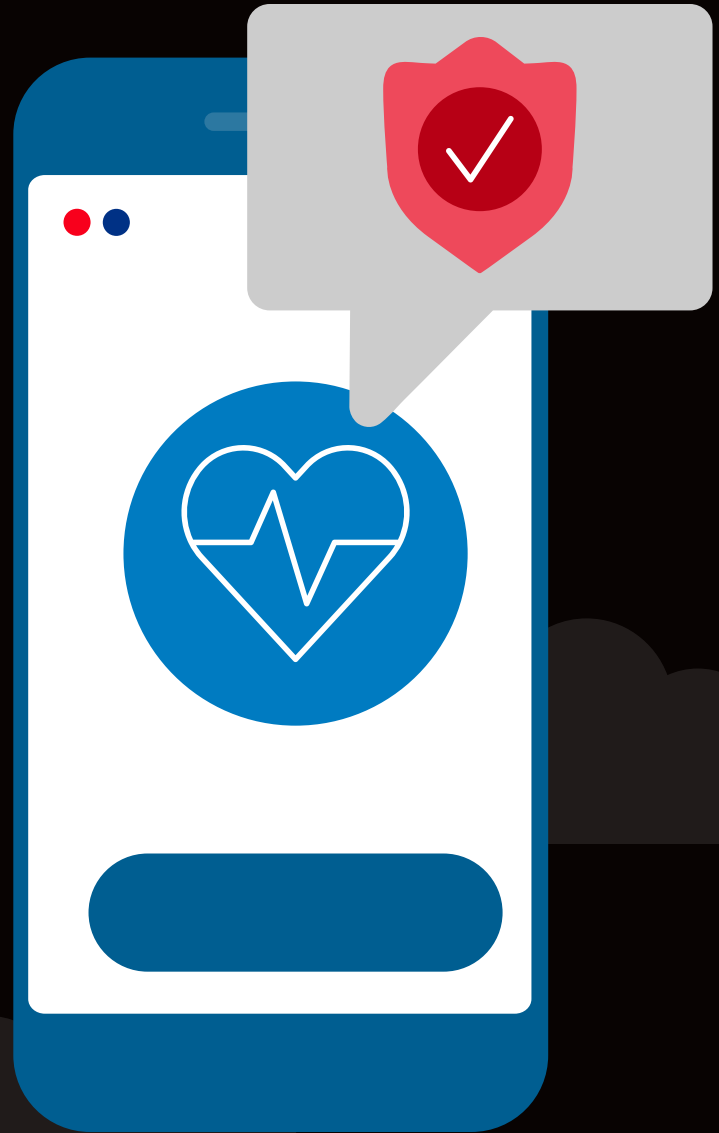


# Protect Healthcare Data and Operations with F5 and AWS

Prevent downtime and maintain compliance with solutions to keep your apps secure, fast, and available in the cloud.



## Contents

<b>3</b>	<b>Balancing Modernization and Security in the Cloud</b>
<b>4</b>	<b>Understanding the Impact and Causes of Outages</b>
<b>5</b>	<b>Add Protection and Performance Without Complexity</b>
<b>6</b>	<b>Secure Healthcare Apps</b>
<b>7</b>	<b>Prevent App Misconfiguration</b>
<b>8</b>	<b>Increase App Availability</b>
<b>9</b>	<b>Protect Healthcare Data and Operations with F5 and AWS</b>

# Balancing Modernization and Security in the Cloud

Healthcare IT is evolving, with 90% of organizations expected to adopt cloud computing by 2025.<sup>1</sup> Already, more than 70% of healthcare organizations are using not just one, but multiple public clouds.<sup>2</sup> Cloud has allowed hospitals and clinics to reduce their reliance on legacy hardware and software, as well as improve financial planning and costs.<sup>3</sup>

However, while the speed, flexibility, and scale of cloud are helping to modernize healthcare IT, cloud decision makers are still concerned about security, privacy, and compliance of their sensitive data.<sup>4</sup> Properly processing, maintaining, and storing protected health information in the cloud is necessary to comply with HIPAA.

**In 2023, more healthcare records were exposed or stolen in data breaches than ever before.<sup>7</sup>**

Not only must your cloud services be compliant, but you must also adequately secure data in your growing attack surface. Healthcare is a frequent target for cyberattacks, and a record-high 133 million healthcare records were exposed or stolen in 2023.<sup>5</sup> The total number of data breaches actually decreased in 2023, but there were more large-scale breaches that exposed millions of records. This indicates that when threat actors gain access, they are exfiltrating larger sets of patient records.

The financial fallout of these attacks can be significant, as the average cost of a healthcare data breach was nearly \$11 million in 2023.<sup>6</sup> This figure includes losses, remediation, fines, and other associated costs. But financial losses are just one part of the damage.



# Understanding the Impact and Causes of Outages

Security incidents and data breaches have a negative impact on patient outcomes. According to research, outages due to ransomware lead to delays in treatment, procedure cancellations, and ambulance diversions.<sup>8</sup> Outages make it hard for staff to access medical records, orders, or prescription data, increasing work for staff and risk for patients.

The vast majority of healthcare breaches in 2023 were caused by a cyberattack or other IT incident, with stolen data most frequently located on a network server.<sup>10</sup> Top ransomware attack vectors included vulnerabilities (both zero-day exploits and known unpatched systems) and brute-force attacks,<sup>11</sup> while basic web application attacks, system intrusion, and miscellaneous errors were the top patterns seen in data breaches.<sup>12</sup> Electronic health records (EHRs) are the most vulnerable system.<sup>13</sup>

The potentially dire outcomes of an outage require healthcare IT teams to take extra measures to defend against downtime.

## Case Study: The Impact of Ransomware

In 2022, a ransomware attack against a large U.S. hospital network went undetected for nearly 20 days. Resulting IT outages and EHR downtime required switching to paper records and disrupted patient care, including delays, cancellations, and diversions. Payroll systems and patient portals were also offline.

The incident took nearly six months to fully investigate and resulted in over \$100 million in estimated damages.<sup>9</sup>





# Add Protection and Performance without Complexity

While increasingly sophisticated attacks and complex hybrid or multicloud infrastructure have made defending healthcare data and operations difficult, F5 and AWS have solutions to protect patient care.

AWS offers a number of HIPAA-compliant solutions for providers, payors, and healthtech organizations. If you wish to run workloads securely in the cloud, AWS CloudFormation templates can create and provision an environment made of HIPAA-eligible services.

F5 application delivery and security solutions for AWS help ensure your apps are available and secure to maintain quality ongoing care. Protect against threats in the OWASP Top 10 and distributed denial-of-service (DDoS) attacks that put your organization and patients at risk. Consistent policies and unified management decrease the complexity of hybrid or multicloud environments.

## Using Epic Systems for Your EHR?

Epic customers can deploy apps on AWS for fast scalability and reduced operational costs. Whether your Epic apps reside solely on AWS alone or are part of a hybrid environment, F5 can add consistent security and performance wherever needed. Both AWS and F5 work with Epic to create validated solutions to optimize and secure your healthcare apps.

**F5 and AWS help address three common app challenges:**



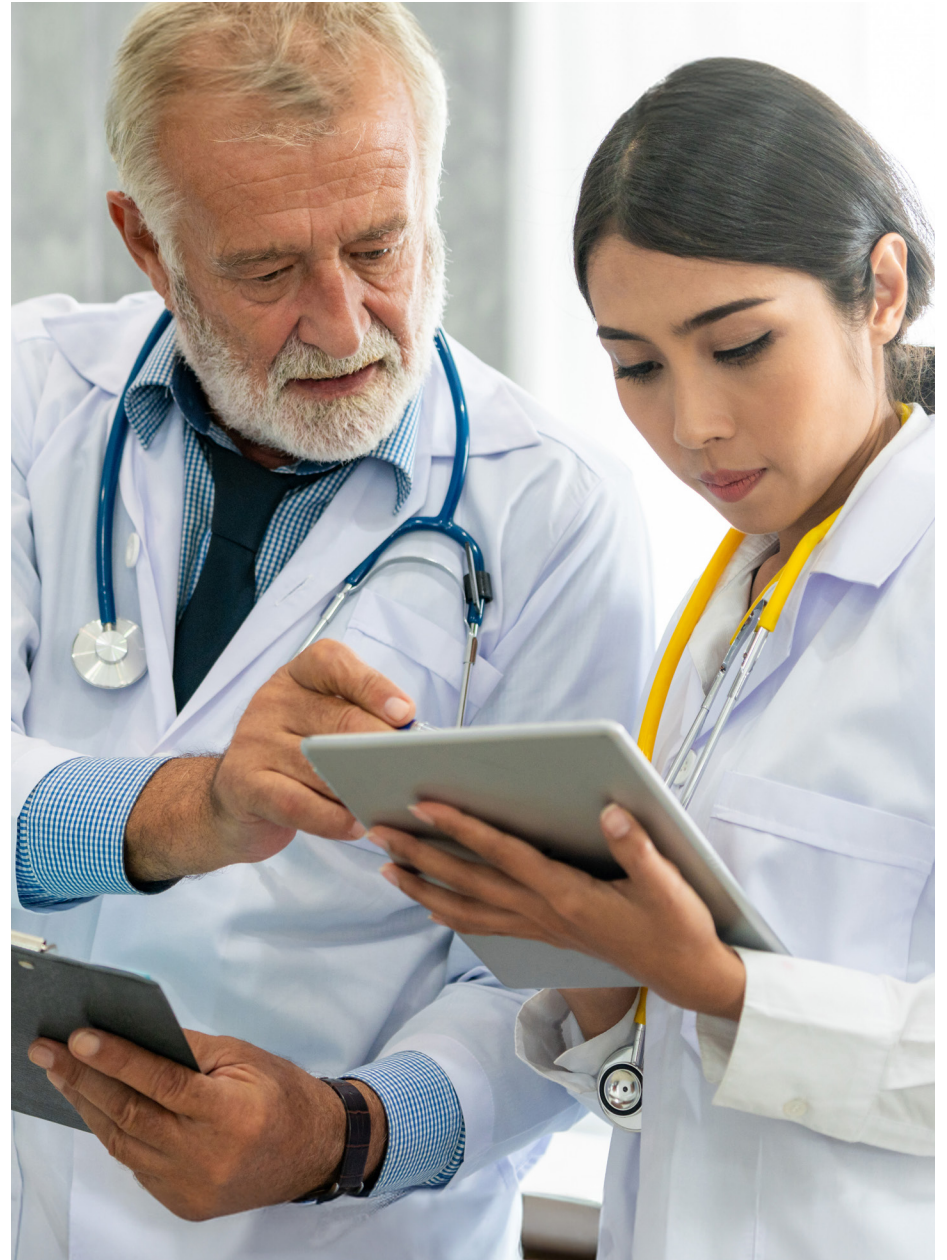
**Security**



**Misconfigurations**



**Availability**





## Secure Healthcare Apps

Whether you've built a unified view of patients from multiple sources or used AWS to transform data into insights, sensitive data must be kept secure from human and automated attackers. You need comprehensive protection from threats that range from zero-day vulnerabilities to automated attacks.

F5® BIG-IP® Advanced WAF® protects applications and the APIs that connect them with behavioral analytics to identify threats that can evade signature-based detection. Secure your apps deployed on AWS or on premises with consistent security policies managed from a single console to improve your security posture and reduce complexity.

F5 also offers protection specifically for Epic applications with pre-built, validated WAF policies and templates that can be customized for your specific needs. Use F5 Application Services Templates (FAST) to automate the configuration of BIG-IP Advanced WAF in your AWS environment. With quick and easy configuration, administrators can take advantage of best practices and rapidly deploy new Epic applications with less effort.

In addition, F5 BIG-IP provides network isolation to separate application web front ends from back-end databases for greater protection of sensitive data. You can also adjust app authorization levels based on the user and location to maintain compliance.

### Benefits of F5 Security on AWS

- Increased detection with behavioral analysis and machine learning
- Granular policy controls down to the microservice level
- Dashboards to easily understand security posture and compliance
- Leaked credential check to prevent unauthorized access
- Bot defense to rapidly discover and block malicious bots



# Prevent App Misconfiguration

Manually configuring new apps, especially when deploying across different environments, can be complicated and time consuming for IT staff. Multiple variables increase the risk of errors that could result in a security incident or downtime. Accidental misconfiguration can also cause configuration drift or poor app performance.

Reduce the risk for your EHR and other Epic applications with pre-built templates that follow best practices and industry standards. FAST templates for BIG-IP can deploy Epic applications in just minutes and are regularly updated to ensure the best performance. They require minimal variables to reduce the chance 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.

## Benefits of F5 Application Services Templates

- Secure and compliant apps that follow best practices and industry standards
- Consistent applications everywhere with standardized configuration
- Lower risk of error with minimal template variables exposed to the user
- Faster, efficient deployments with automation





## Increase App Availability

Your healthcare apps must always be fast and available to support your staff in an emergency. When apps run slowly or are unavailable, it creates extra work and frustration for medical staff and patients. For example, an EHR outage requires relying on paper backups that can impact quality of care and significantly slow down medical staff.

F5 BIG-IP application delivery services let you scale application traffic on AWS or on premises using the same policies and management for improved consistency. By optimizing network traffic, apps remain fast and accessible on your AWS, hybrid, or multicloud environment. BIG-IP monitors service health to steer traffic to the best available server or automatically fail over to a backup location if needed.

Built-in DNS security blocks malicious communications that could slow performance or increase infrastructure costs. SSL offloading helps speed server performance by having BIG-IP manage encryption and decryption, which can also allow your security tools to inspect encrypted traffic without causing a slowdown.

BIG-IP can be deployed on-premises with hardware or on AWS and other clouds with virtual editions for consistent policies and improved performance everywhere.

### Benefits of F5 Application Delivery Services

- Always-available apps with intelligent traffic management, global load balancing, and automated failover
- Improved server performance with encryption offload
- Faster app load times with on-demand scaling
- Better user experience with app health and performance monitoring



# Protect Healthcare Data and Operations with F5 and AWS

F5 offers application delivery, security, and networking across the entire hybrid cloud estate to provide reliable and secure apps and services on AWS or anywhere else you need them. The long-standing partnership between F5 and AWS means you can expect solutions that work together seamlessly to help you maintain patient privacy and quality care.

**Ensure your clouds, apps, and services are always:**



**Secure**



**Available**



**Fast**

**Learn more about F5 solutions for AWS at [f5.com/aws](https://f5.com/aws)**

## **The F5 and AWS Partnership:**

- 10+ years of collaboration
- Over 1,000 joint customers
- Competencies for containers, networking, and security
- Service validations for AWS WAF, Amazon CloudFront, AWS Outposts, and Linux
- Over 20 AWS certifications

# Appendix

<sup>1</sup>DuploCloud, [70% of Healthcare Businesses Have Adopted Cloud Computing: DuploCloud Report](#), Feb 2023

<sup>2</sup>Forrester, [The State Of Cloud In Healthcare, 2023](#), May 2023

<sup>3</sup>AWS, [Accelerate healthcare transformation with cloud solutions](#), Jun 2023

<sup>4</sup>Forrester, [The State Of Cloud In Healthcare, 2023](#), May 2023

<sup>5</sup>HIPAA Journal, [December 2023 Healthcare Data Breach Report](#), Jan 2024

<sup>6</sup>IBM, [Cost of a Data Breach Report 2023](#), Jun 2023

<sup>7</sup>HIPAA Journal, [December 2023 Healthcare Data Breach Report](#), Jan 2024

<sup>8</sup>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

<sup>9</sup>Office of Information Security and Health Sector Cybersecurity Coordination Center, [Ransomware & Healthcare](#), Jan 2024

<sup>10</sup>Fortified Health Security, [2024 Horizon Report](#), Jan 2024

<sup>11</sup>Office of Information Security and Health Sector Cybersecurity Coordination Center, [Ransomware & Healthcare](#), Jan 2024

<sup>12</sup>Verizon, [2023 Data Breach Investigations Report](#), Jun 2023

<sup>13</sup>Mejía-Granda CM, et al. [Security vulnerabilities in healthcare: an analysis of medical devices and software](#), Medical & Biological Engineering & Computing, Jan 2024

# ABOUT F5

## BRINGING A BETTER DIGITAL WORLD TO LIFE

F5 is a multicloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure and optimize apps and APIs anywhere—on premises, in the cloud, or at the edge. F5 enables organizations to provide exceptional, secure digital experiences for their customers and continuously stay ahead of threats.

For more information, go to [f5.com](https://f5.com). (NASDAQ: FFIV).

Learn more about F5 Distributed Cloud Multicloud Networking at

[f5.com/solutions/use-cases/multi-cloud-networking](https://f5.com/solutions/use-cases/multi-cloud-networking).

