



Delivering Digital Health Services through Secure, Adaptive Apps

The World Health Organization (WHO) claims digital health will be valued and adopted if it is accessible, enhances efficiency and sustainability, strengthens and scales care, and is in a system that respects the privacy and security of patient health information.¹ An increasingly digital-first user base is putting pressure on healthcare organizations to provide better patient experiences without compromising the safety of their electronic health records and healthcare transactions.

Responding to this need, healthcare organization CIOs have flagged cloud infrastructure as their second-highest investment area in 2022.² The shift to cloud has also increased the use of other advanced capabilities, such as cloud-native application development and deployment, with CIOs reporting that 20–40% of business processes have been automated.³

Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains.⁴

F5 and Google Cloud have a vision for protecting and powering adaptive applications that can meet the digital demands of the healthcare sector by providing modern patient-centric services that protect personal health information from compromise, fraud, and misuse. Automatically respond to new cyberattacks, updates to security posture, performance degradations, and changes in the environment. Deliver extraordinary digital patient care through adaptive applications that grow, shrink, defend, and gain insights to quickly evolve to changing environments, keeping patient data safe and maintaining regulatory compliance at every turn.



Maintain Operating Integrity

Safely store and analyze sensitive, personally identifiable information with multiple layers of physical and logical protection.

Block automated bot traffic to reduce the burden on infrastructure and stop attempts to compromise the integrity of critical information.



Modernize and Secure Your Apps

Modernize your existing applications, build new innovative apps, and run them securely in hybrid or multi-cloud environments.

Guard against common vulnerabilities and mitigate emerging exploits that target open source software and security misconfigurations across clouds.



Stop Fraudsters in Their Tracks

Stop most fraud downstream before it happens by detecting and removing automated bots and human attackers.

Bring security and fraud teams—and data—together, enabling fraud investigators to focus on high-value, upstream fraud investigations instead of false positives.



Deliver Care with Confidence

Utilize artificial intelligence (AI) powered recommendations and personalization while automatically adapting to changing attack tactics without inserting user friction to ensure timely care delivery and customer satisfaction.

Monitor every transaction for signs of fraud or risky behavior to gain comprehensive insights.

For more information, please [visit f5.com](https://www.f5.com).

Source:

1. World Health Organization, [Global strategy on digital health 2020-2025](#), May 2021

2. Evanta, [10 CIO Trends in 2022](#), February 2022

3. IBM, [2021 CIO Study: The CIO Revolution](#), November 2021

4. Gartner, [7 Top Trends in Cybersecurity for 2022](#), April 2022