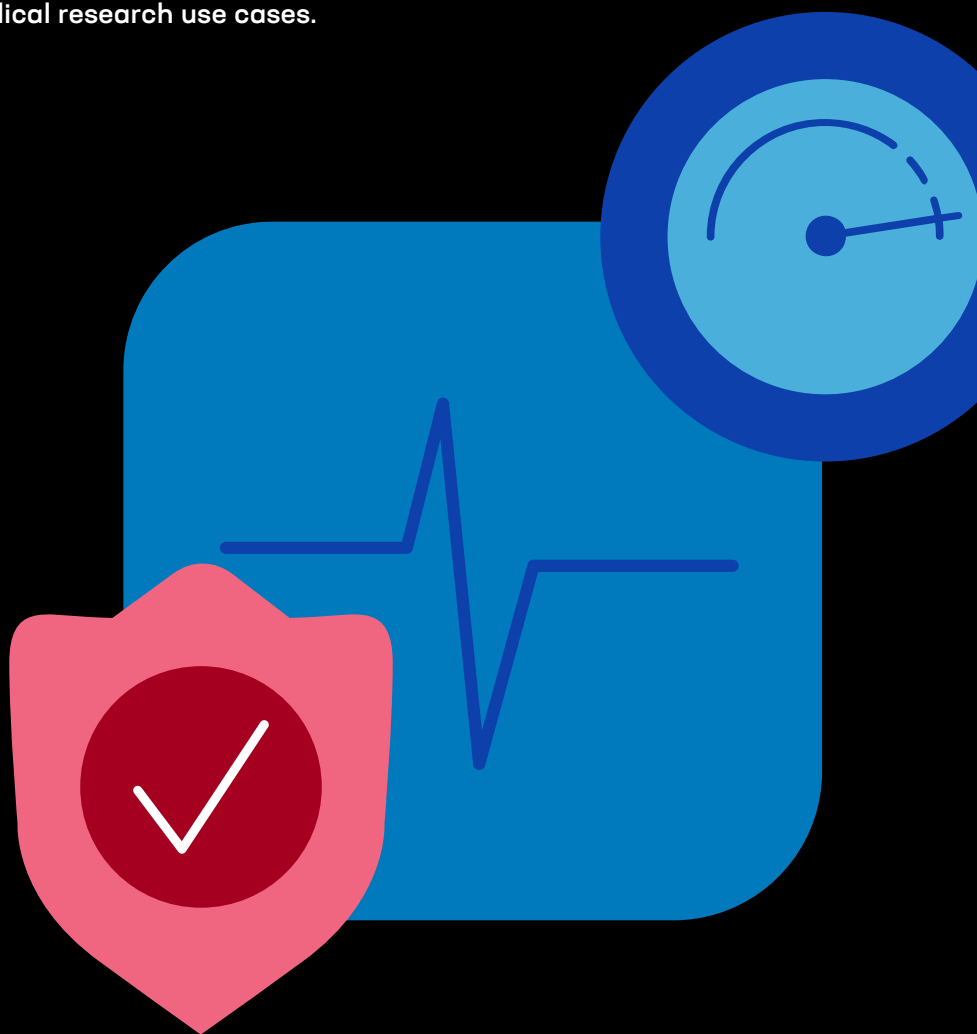


Protect global healthcare app delivery with F5 and Equinix

Secure telehealth, safeguard data exchanges, and ensure compliance with F5® Distributed Cloud Services on Equinix Network Edge. Eliminate infrastructure complexity while providing continuous, reliable, and high-performance applications for vital healthcare and medical research use cases.



Key benefits

Seamless global deployment

Easily deploy infrastructure close to patients, providers, partners, and staff, leveraging Equinix's global footprint for consistent performance while reducing complexity and time to market.

Scalability and compliance

Ensure scalability and regulatory compliance while managing access control and data governance with location-specific data policies to address varying compliance requirements without costly separate infrastructure.

Improved collaboration

Accelerate clinical research and trials with secure, governed access to patient or research data through private connectivity and segmented network access that maintains full audit trails and compliance controls.

Enhanced user experience

Provide low-latency application access for providers, researchers, and patients without compromising security or regulatory compliance.

Unified security and networking

Leverage F5 Distributed Cloud Services for security, networking, and application delivery across distributed environments.

Accelerated time-to-market

Deploy application environments in new regions with just a few clicks, bypassing lengthy traditional hardware procurement cycles.

Healthcare application deployment is complex

As healthcare becomes increasingly digital, IT departments and applications teams are faced with evolving challenges, such as supporting and securing telehealth services and EHRs to avoid disrupting patient care. Regulations including HIPAA and GDPR complicate data management, as do a growing number of regional data privacy laws.

To support patients, providers, and research, healthcare organizations need to provide secure, low-latency access to applications and support global data sharing without violating privacy regulations.

Ultimately, healthcare IT departments need to protect a complex and widespread environment while enabling secure access, which often requires specialized infrastructure that adds cost and management overhead.

Simplify operations with F5 and Equinix

By combining F5® Distributed Cloud Services and Equinix Network Edge, healthcare organizations can reduce operational complexity and securely connect public clouds, private data centers, and edge sites around the world.

F5 Distributed Cloud Customer Edge (CE) software operates as a virtual network function (VNF) that is deployed on Equinix Network Edge. This solution extends Distributed Cloud Services, including app and API security, intelligent load balancing, and secure multicloud networking, into any environment where applications are hosted, creating a unified control plane to reduce overall complexity.

Equinix's extensive global footprint allows you to deploy Distributed Cloud CE wherever it's needed without requiring physical infrastructure, which reduces complexity and improves application performance. Equinix Fabric adds secure, private, software-defined interconnections between distributed infrastructure, cloud providers, and key partners for low-latency, high-speed connectivity without the security and compliance pitfalls of the public Internet.

Key features

Virtual network functions

Deploy F5 services as pre-built VNFs without physical hardware on Equinix Network Edge.

Distributed Cloud

Customer Edge

Extend Distributed Cloud Services to any environment where applications are hosted to provide security, traffic management, and networking with centralized management.

Equinix Fabric connectivity

Enable software-defined interconnections between distributed infrastructure, cloud providers, and partners.

Multi-environment control plane

Reduce complexity with a unified control plane and consistent policies across hybrid multicloud environments, including the ability to apply location-specific data policies.

Integrated security services

Protect apps with built-in WAF, bot defense, DDoS protection, and API security while maintaining strict governance standards and audit capabilities.

Achieve your healthcare objectives

Power secure telehealth

Support protected, reliable, high-performance telehealth services at the edge to deliver a better experience to providers and patients. Together, F5 and Equinix equip you to rapidly deploy essential care applications without compromising security.

Through Distributed Cloud CE and Equinix Network Edge, you can enable continuous service availability while protecting sensitive data from security threats with centralized policies and consolidated management across all delivery points. The pre-built integration significantly reduces operational burden, allowing your teams to focus on enabling better outcomes rather than infrastructure management. This approach helps your organization quickly adapt to changing needs and save costs without increasing cyber risk.

Protect patient data exchanges

Safeguarding sensitive data as it's shared across globally distributed care partners is typically difficult for security and IT teams, involving multiple point products spread across various locations. Distributed Cloud CE and Equinix Network Edge enable you to provide secure medical data exchanges while maintaining compliance with regulations such as HIPAA and GDPR. Your team can create segmented, private, low-latency connections for sharing patient data with authorized care providers and other partners. These protected exchanges can help you meet data sovereignty requirements while enabling protected collaboration across global locations.

Enable secure global research

Distributed Cloud CE and Equinix Network Edge also provide capabilities to securely share data between research institutions, hospitals, and pharmaceutical partners. Your team can create protected environments for sharing anonymized patient data and research findings across organizational and global boundaries while ensuring data security and regulatory compliance.

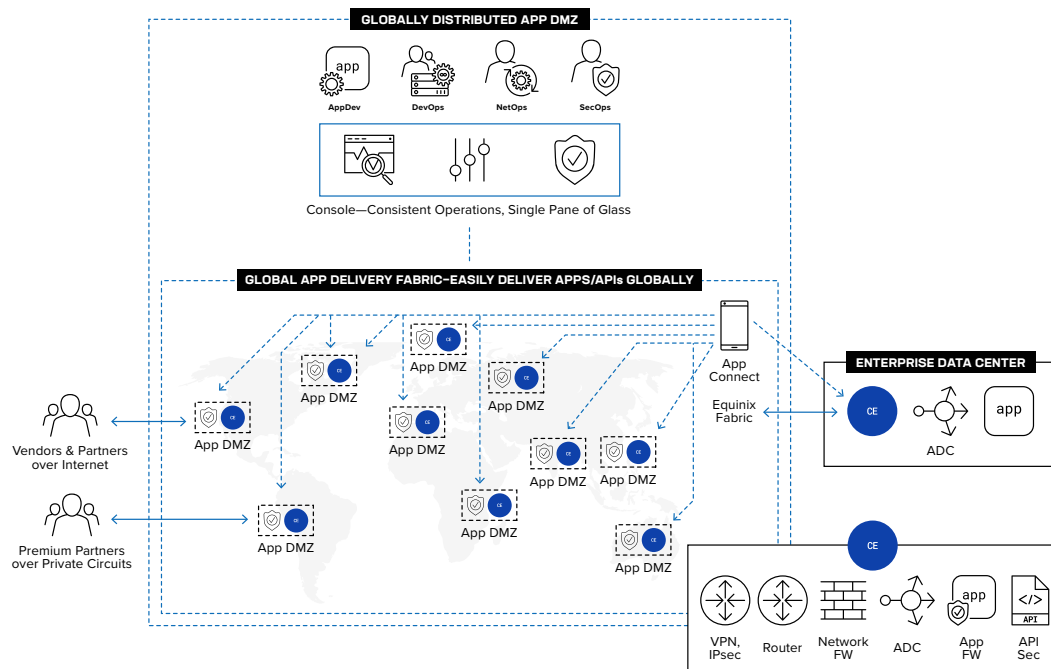


Figure 1: Seamlessly deliver and secure apps globally with centralized policies and consistent operations.

Unlock compliant worldwide expansion

For healthcare organizations operating on a global or nationwide scale, F5 and Equinix enable rapid deployment of regional-specific services that comply with local regulatory requirements. Centralized management allows you to deploy identical security configurations across multiple jurisdictions with location-specific data policies, ensuring consistent security and addressing varying compliance requirements without having to maintain costly infrastructure in each region.

Support global healthcare applications with seamless deployment and connectivity

Overcoming the challenges of modern healthcare application deployment requires innovative solutions that ensure performance and security without adding complexity. Distributed Cloud Services and Equinix Network Edge allow healthcare organizations to efficiently scale applications globally, maintain regulatory compliance, and manage access securely. This integrated approach accelerates digital transformation and provides the agility necessary to adapt to evolving demands, ensuring a high-performance, globally distributed application environment that meets the unique needs and strict regulations of the healthcare industry.

Learn more about the F5 and Equinix partnership at f5.com/equinix.

