SOLUTION OVERVIEW

F5 U.S. Federal Application Modernization Solutions

Fueled by initiatives like the Technology Modernization Fund, agencies need to accelerate application development and deployment without sacrificing security–improving mission agility, efficiency, and effectiveness. F5 can help.

KEY BENEFITS

Modern Architectures
Modern delivery designs are innovative and fluid. We offer adaptive API gateway and security solutions that support virtually any deployment model.

DevOps / AppDev Friendly
Drive business velocity by integrating into automated deployments, with the tools your teams are already using.

Shift Security Left
Application security is intrinsically integrated into the application development lifecycle, resulting in less friction between security and app dev teams.

Highest Security Efficacy
F5 protects apps against the most sophisticated attacks—securely accelerating digital transformation and protecting the mission.

Automated Protection
F5 solutions adapt and maintain full efficacy, even as attackers retool and evolve to overcome countermeasures, without compromising the overall user experience.

Tight budgets, growing cybersecurity concerns, and the challenge of maintaining legacy applications and infrastructures are overloading traditional IT resources in federal agencies. Many agencies today are under increasing pressure to keep costs low and serve a growing number of users, while managing and protecting a massive amount of data. As a result, government agencies are finding that the legacy applications they've relied on to support their mission and operations are now unable to fully support the business requirements of innovation, agility, and efficiency.

Furthermore, dated and complex federal network architecture and app development and deployment processes make it difficult for agencies to deliver the kind of digital experiences citizen and government employees expect from consumer-grade apps. Forrester data indicates that government agencies have listed "improve the experience of our employees" (20%) and "improve the experience of our customers" (16%) as top business priorities over the next 12 months.[1]

If they don't keep up with growing demands from civilians and government employees for positive digital experiences, federal agencies may not be able to maintain mission effectiveness.

With F5, federal agencies can streamline application modernization and reduce complexity by supporting rapid app innovation, integrated security, and accelerated app deployment. F5 solutions help federal agencies improve mission agility, efficiency, and effectiveness, and keep pace with evolving citizen and employee demands for positive digital experiences.

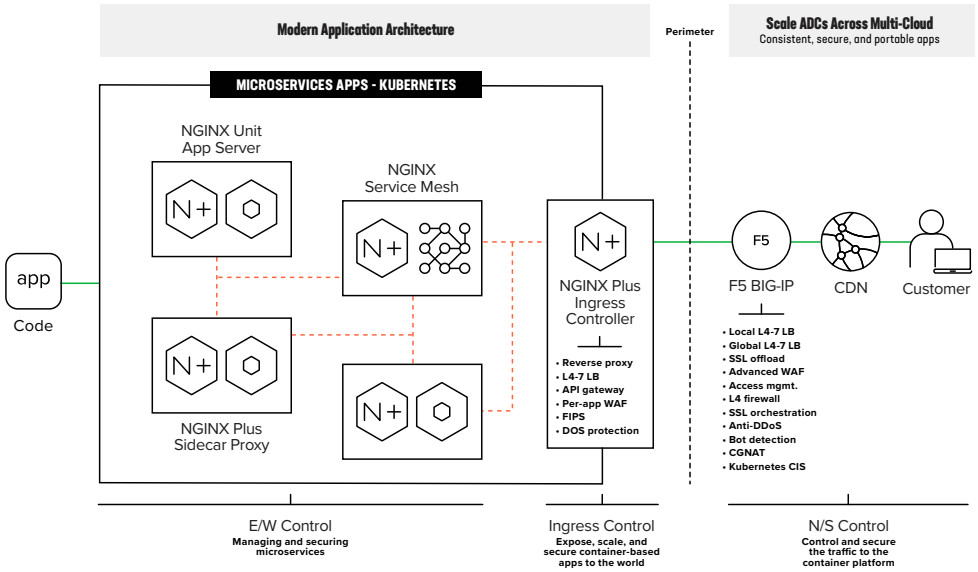

Figure 1: Protect and scale Kubernetes across your application portfolio with the reliability you expect from F5.

IN TODAY'S FAST-CHANGING WORLD, FEDERAL AGENCIES THAT CHOOSE NOT TO MODERNIZE THEIR LEGACY APPLICATIONS MAY BE PUTTING THEIR MISSION AT RISK.

The Importance of Rapid Application Development and Deployment

Evolving mission modernization needs at federal agencies call for accelerated application development and innovation. F5 solutions support this effort by integrating performance, security, and compliance into app development and DevOps pipelines, allowing agencies to develop and deploy applications at speed. This equips your agency to:

- Do more with less and modernize your apps to ensure they run faster and more efficiently.
- Reduce total cost of ownership for your apps by reducing the number of legacy apps and the time and resources your IT team devotes to managing and maintaining them.
- Make apps more scalable and easier to update by reducing deployment time from months to minutes.
- Mitigate security risk more easily and effectively.
- Save money by eliminating the need to purchase new hardware every time you need to update your system.
- More easily manage cloud migrations and deployments, and avoid cloud vendor lock- in.

Accelerate App Innovation with F5 Through DevOps Practices and Microservices Architecture

Traditional, or monolith, applications are connected to siloed platforms that block modern development processes. As monoliths grow in size and scope, their code typically becomes tightly coupled, making them extremely difficult to extend or change. The interconnected modules of monolithic systems not only slow development, they're at high risk of failure every time a new feature is deployed.

To succeed in the future, continuous delivery, constant experimentation, and both civilian and employee feedback are crucial. For many, this means moving away from monolithic architectures towards microservices. If moving to microservices is the right choice, then choosing the right implementation is also critical.

The F5 and NGINX vision is to simplify the journey to microservices. As agencies implement a DevOps approach to application development and delivery, the tools, stack, and interoperability can become highly complex. The F5 and NGINX application platform helps reduce this complexity by consolidating common functions down to far fewer components, making application infrastructure scalable and more manageable. Ultimately, this leads to both low latency and more secure applications.

To help accomplish this, F5 and NGINX uniquely provide several key components to the microservices architecture including containerized applications, load balancing, ingress control, API gateway, API management, security, management of encryption-in-transit, and more.

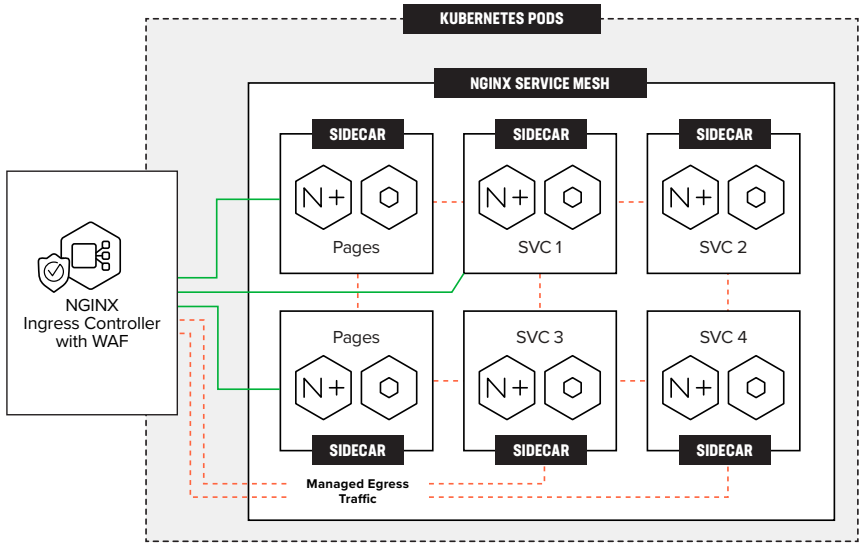

Figure 2: Secure and manage cloud-native, containerized apps

F5 and NGINX streamline the journey to microservices and enable agencies to:

- Use F5 solutions to protect and optimize containerized applications, without introducing slowdowns or security risks.
- Leverage a supported platform, reduced complexity, integrated security, advanced capabilities, and increased scale and performance.
- Rely on NGINX as the world's most widely deployed ingress controller for Kubernetes[2], and reduce the complexity of clusters by consolidating traffic routing, security services, authentication, encryption, and API gateway functions.
- Monitor Kubernetes environments with NGINX Plus Ingress Controller to automatically identify new container applications and make necessary changes to the NGINX configurations dynamically for automated ingress and egress routing for new or changed applications.

Why Secure Application Development Is so Important

Speed cannot come at the expense of security. F5's solutions, including NGINX and Shape Security, incorporate security throughout the development process, from beginning to end. Agencies can even address vulnerabilities before deployment, resulting in more secure applications without compromising innovation.

KEY FEATURES

- Native integration in application development frameworks improves time to market and reduces friction
- Protection from well-known and emerging threats reduces risk and accelerates app modernization
- Support for all architectures, form factors, deployment modes, and compliance mandates provides flexibility to support all applications
- Out-of-the-box protection from application vulnerabilities reduces risk and remediation costs
- Dynamic signature feeds to block emerging threats allow security to adapt to the threat landscape
- Automated policy deployment improves effectiveness by implementing and stabilizing security controls earlier in the software development lifecycle
- Integration into the CI/CD pipeline reduces friction between development and security teams
- Declarative API simplifies policy deployment and maintenance by abstracting complexity and reducing developer overhead
- API-driven deployment and maintenance simplifies policy management and change control across multiple architectures and clouds

Employ DevSecOps-Integrated Security Into CI/CD Pipeline

Protect your users, organization, and mission from existing and emerging threats by embedding security into the application development and deployment process and ensuring compliance with federal security guidelines from NIST and DISA.

- Automate security and performance policies into your code pipeline to keep things running smoothly and securely across clouds; consistent policies mean fewer gaps and stronger security.
- Manage and secure APIs—Securely manage APIs across any data center or cloud using a simple, fast, and scalable multi-cloud architecture.
- Get app protection in any architecture—safeguards that will stand up to a range of ever-evolving attack types.
- Virtually eliminate post-deployment security vulnerabilities that increase development and deployment times by baking security into app development.

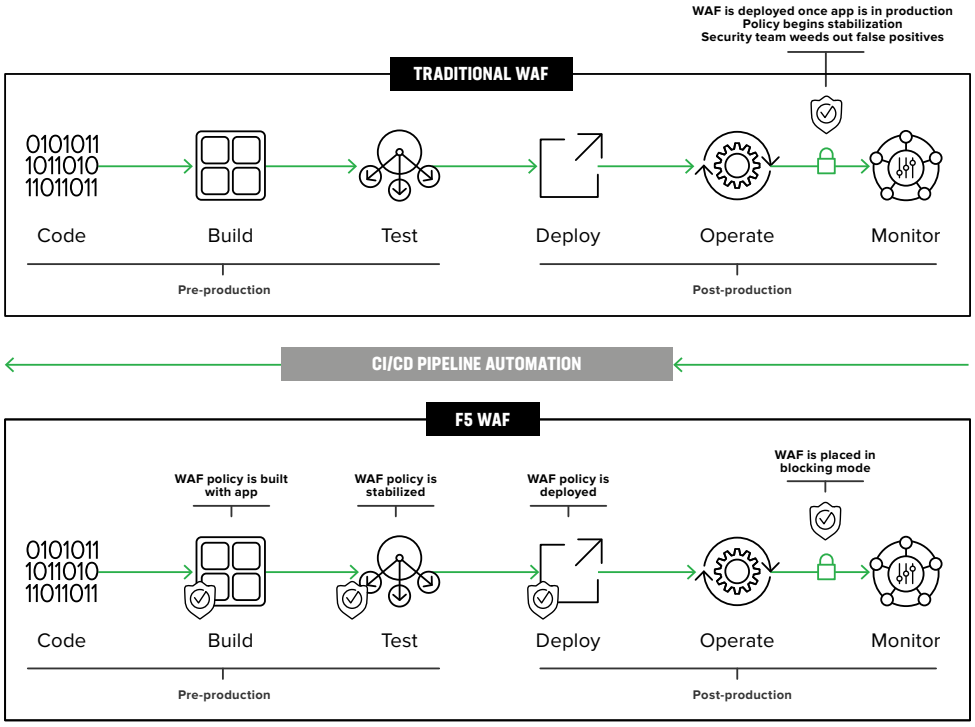

Figure 3: CI/CD pipeline automation can improve time to market while reducing risk and producing better business outcomes

Conclusion

F5 U.S. federal solutions help agencies accomplish their mission through application modernization efforts. Migration support from legacy applications into modern architectures reduces the total cost of ownership, and increases the speed of application innovation—keeping pace with citizen and employee demands for fast and secure digital experiences.

U.S. federal agencies are endlessly targeted by malicious attackers. F5 offers the highest protection from both well-known and emerging threats—reducing your agency's risk, protecting your apps from sophisticated attacks, and securely accelerating application modernization.

F5 solutions offer support for all architectures, form factors, deployment modes, and compliance mandates, providing flexibility to support applications. Ultimately, these solutions promote application portability and provide the agility your mission requires. You're never locked into the constraints of any single environment, whether it's cloud-hosted or on-premises infrastructure. Our application modernization solutions are here to help you deliver superior user experiences that are secure, scalable, and always available.

To learn more, explore F5 application modernization solutions or contact your U.S. federal F5 representative.

[1] Source: Forrester, The Promise (And Perils) Of Customer-Focused Government Technology Transformation , 2019, found at https://www.forrester.com/report/The+Promise+And+Perils+Of+CustomerFocused+Government+Technology+Transformation/-/E-RES162676?objectid=RES162676

[2] Cloud Native Computing Foundation Survey 2020, found at https://www.cncf.io/wp-content/uploads/2020/11/CNCF_Survey_Report_2020.pdf

DC0721 | OV-300USFED-702850058