SOLUTION OVERVIEW

Increase Application and Infrastructure Resiliency

Deliver high-performing, adaptive applications with reliable and automatable cross-platform security and infrastructure solutions from F5.

KEY BENEFITS

- Implement cloud-agnostic performance solutions that provide common infrastructure-as-code configurations, no matter what platform you rely on.
- Get the flexibility you need, with F5 and NGINX offering more functionality in more application deployment models than any other cloud-native or third-party solution provider.
- Leverage F5's large developer community to improve on your BIG-IP solutions or use the world's open source communities to improve your NGINX deployments and performance services.
- Build adaptive infrastructure at node, availability zone, perimeter, and public namespace with F5's complete suite of security and application service solutions.

Disaster recovery alone isn't enough when customer experience is on the line. Disaster recovery plans used to measure how many hours an application could be down and still be considered reliable. Today's modern applications don't have such luxuries; disruptions guarantee poor customer experience and erode customer trust. Building resiliency beyond code—into security and infrastructure—boosts flexibility. Applications can adapt with changes, both planned and unintended, at scale to ensure performance meets customer and business demands, while remaining secure and reliable.

The technology industry measures a 99.99% available application to be unavailable 52.6 minutes per year, or 4.38 minutes per month. Today's connected customer will respond even faster on social media when they can't use your application. Recovery costs, data loss, reputational damage, and permanent customer loss are all consequences of unplanned application downtime or disruption.[1]

Applications are your primary tool for engaging customers, and customer loyalty and the bottom line directly reflect their digital experiences. Research shows that 32% of all customers would stop doing business with a brand they loved after just one bad experience.[2] Additionally, customers share bad experiences almost as frequently as they share good experiences. In another survey, 57% of customers said they stopped buying from a company because a competitor provided a better experience. And 62% shared their negative experiences with others.[3]

Customer sensitivity to unreliable or inconsistent applications, combined with distributed services and infrastructure in multiple clouds or on-premises, create a complicated recovery plan in case of failure or degraded performance. Deploying to one cloud can be complex enough, but considering most enterprises deploy to two or more cloud providers, resolving problems becomes its own complicated task. Building resilient security and infrastructure to match flexible software deployments provides reliable service that a disaster recovery plan simply cannot accomplish on its own.

57% OF SURVEYED CUSTOMERS STOPPED BUYING FROM A COMPANY BECAUSE A COMPETITOR PROVIDED A BETTER EXPERIENCE; 62% SHARED THEIR NEGATIVE EXPERIENCES WITH OTHERS.[3]

Complexity Will Increase as Applications Grow

The complexity of applications hosted on-premises or in multiple clouds, plus increasing demand for cross-platform reliability, demands applications that can adapt to environmental and behavioral changes when deployed. While development teams enjoy measuring success with deployment-focused performance indicators, studies show that "security and reliability serve as a baseline indicator for trustworthiness."[4] And the same study shows that a customer's digital experience goes further with a company they can trust.

A recent cloud study found that 67% of respondents don't rely on multi-cloud tools, which means they face increased complexity in seeing and managing their cloud performance and availability.[5] Meanwhile, 45% of respondents in another survey indicated challenges with restore reliability, while 44% indicated challenges with backup reliability.[1] With customer data protection and recovery as critical focus areas for digital transformation initiatives, priorities are not always aligned between developers and operational policy.

Build Resilient Security and Application Performance into DevOps Pipelines

STUDIES SHOW THAT "SECURITY AND RELIABILITY SERVE AS A BASELINE INDICATOR FOR TRUSTWORTHINESS."[4]

Software development and fast-paced DevOps pipelines measure success KPIs categorized around availability, performance, and incident reaction times. This pushes developers and DevOps teams to employ more manageable services that rely on native cloud tools and distributed architectures, and potentially leave out operational policies that could impact success. The applications pipeline becomes resilient—able to gracefully detect and respond to problematic variables in customer and software behaviors—but it may lack compliance or data protection mandates requested by digital transformation projects.

Resilient applications and their deployment pipelines don't always address the potential disruptions found outside of software and basic infrastructure functionality, nor do they consistently address larger issues when deployed across multiple platform providers. Cloud services and regions do fail, and data protection and security aren't only a perimeter function.

Identifying where software resilience ends and infrastructure and security resilience needs begin can close the gap between an application that performs well under tolerable circumstances and a fully resilient application. Resilient applications should be able to meet the demands of customer service-level agreements and disaster recovery under digital transformation and enterprise compliance mandates. Including security and infrastructure configurations within application lifecycles can keep architecture flexible and responsive to code changes. Examples include:

- Deploy security features and policy in the same continuous integration and continuous delivery (CI/CD) stream to protect applications as they are deployed, reducing gaps between compliance and feature functionality.
- Deploy traffic optimization and load balancing policies to deploy with code, so performant traffic reaches the appropriate services, preventing unneeded infrastructure expansion to meet artificial demands.
- Leverage modern infrastructure functionality to dynamically update security, load balancing, and traffic optimization configurations as container environments ebb and flow to meet application needs.

RECOVERY COSTS, DATA LOSS, REPUTATIONAL DAMAGE, AND PERMANENT CUSTOMER LOSS ARE ALL CONSEQUENCES OF UNPLANNED APPLICATION DOWNTIME OR DISRUPTION.[1]

- Deploy global server load balancing polices in CI/CD pipelines, which allows you to spin up and bring online entire application regions and respond globally when catastrophic issues arise.
- Standardize common services across cloud and private platforms to reduce policy complexities, minimizing compliance variance and native service limitations that vary by vendor.

The Architectural Components

F5 gives cloud architects, DevOps, and business leaders the tools they need to deploy and maintain resilient multi-cloud or on-premises application security and infrastructure solutions. So, when the unexpected occurs, your applications remain fast and available. And because F5 solutions include flexible APIs, you can deploy update security and infrastructure alongside code deployments.

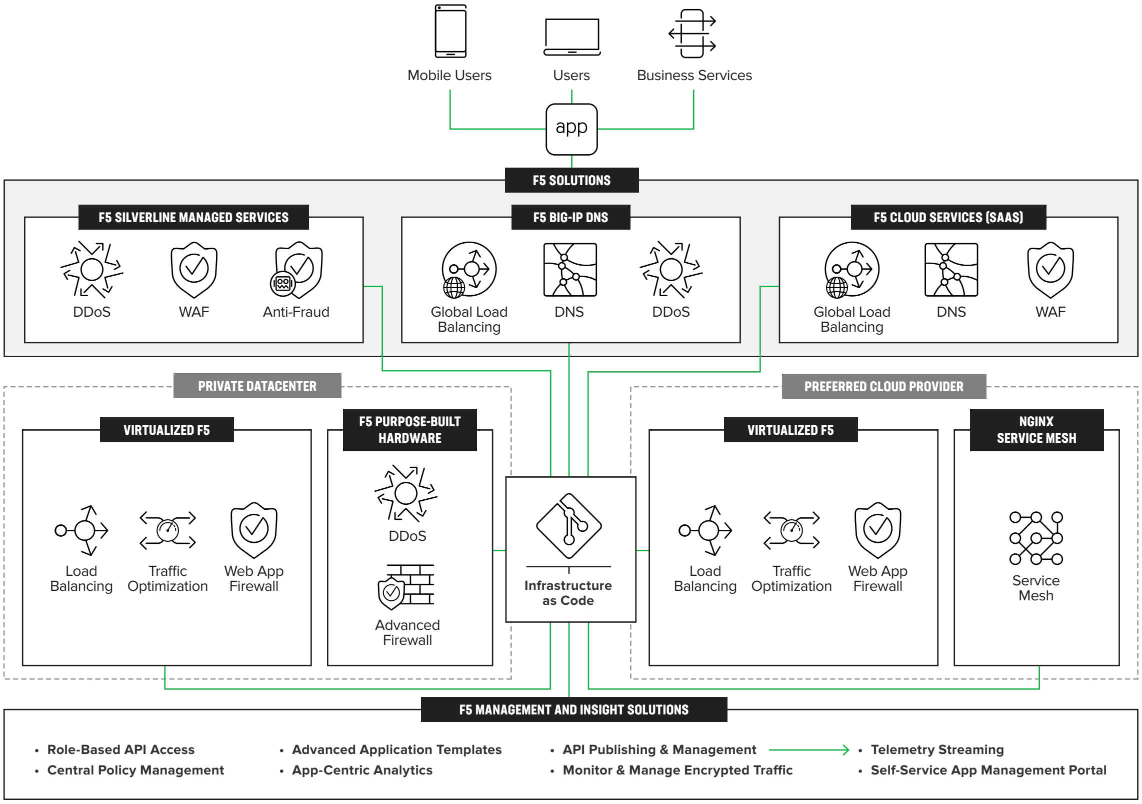

Figure 1: Provide infrastructure-as-code to security, traffic policies, and platform infrastructure in line with application deployments.

F5® BIG-IP® Local Traffic Manager™ (LTM) is the gold standard for application and network traffic management solutions. Inline to your applications' data path, F5 can manage traffic entering and exiting your network, all in real time. BIG-IP LTM optimizes application speed and reliability via both network and application layers. Using real-time protocol and traffic-management decisions based on application and infrastructure conditions, extensive connection management, and TCP and content offloading, BIG-IP LTM dramatically improves application responsiveness.

NGINX Plus builds on the massively popular NGINX Open Source solutions, combining load balancing, web server, and content caching features. NGINX Plus has exclusive enterprise-grade features beyond what's available in the NGINX Open Source offering, including session persistence, configuration via API, and active health checks. Deliver easy-to-implement traditional load balancing features, handle more traffic with resource-optimized web server features, and use the same caching technology that powers the world's largest content delivery network (CDN). Simplify your architecture while reducing costs with the only all-in-one load balancer, API gateway, sidecar proxy, content cache, and web server.

Intelligent F5 solutions can be deployed and updated in coordination with container events. F5 provides a free container integration solution—the F5 Container Ingress Services component for BIG-IP—which runs as a container and subscribes to cluster management events. Container Ingress Services combines event awareness with native container platform tools like config maps and annotations to configure Ingress services via the BIG-IP REST API.

Or add NGINX to your Kubernetes container solution with NGINX Ingress Controller for Kubernetes. This solution provides enterprise-grade delivery services for Kubernetes applications, with benefits for users of both NGINX Open Source and NGINX Plus. With the NGINX Ingress Controller for Kubernetes, you get basic load balancing, SSL/TLS termination, support for URI rewrites, and upstream SSL/TLS encryption. NGINX Plus users also get session persistence for stateful applications and JSON Web Token (JWT) authentication for APIs.

F5 DNS delivery solutions improve the performance and availability of your global applications, allowing behind-the-scenes flexibility in your application deployments. With a feature set that includes multicore scalability, DNS Express, and IP Anycast integration, DNS delivery can handle millions of DNS queries, protect your business from DDoS attacks, and ensure top application reliability for users. Leverage F5's DNS solutions with BIG-IP DNS hardware or virtual editions or through a SaaS model with F5 Cloud Services.

KEY FEATURES

Manage and Deliver Your API Portfolio
Leverage a full API lifecycle management solution that's automation friendly, delivers optimum performance for internal (microservices) and external APIs, and supports multi- and hybrid-cloud environments.

Traffic Optimization
F5's highly optimized TCP/IP stack combines TCP/IP techniques and improvements in the latest Request for Comments (RFC), with extensions to minimize the effect of congestion and packet loss and recovery. Independent testing tools and customer experiences add up to a 2x performance gain for users and a 4x increase in bandwidth efficiency.

Integrate Security Into CI/CD Pipelines
Integrate with common tools like Ansible, Terraform, ServiceNow, and GitLab to match the workflow of the tool you're using.

Advanced App-Centric Configuration
Use role-based access control (RBAC) and self-service to set up security guardrails (not gates), so your teams can manage their apps securely and with agility. Enable multi-tenancy, reusability, simpler configs, and more.

F5 Advanced Web Application Firewall™ combines machine learning, threat intelligence, and deep application expertise to protect your applications from automated and targeted threats. Starting with industry defense against the OWASP Top 10, expand your web application protection to cover unique application behaviors—protection that standard signature and reputation-based solutions can't provide. Deploy security polices to protect your public and private application endpoints, including tools to secure REST/JSON, XML, and GWT APIs.

NGINX App Protect deploys trusted controls close to your apps, protecting against customer-impacting attacks, data theft, sideband or internal attacks, and regulatory non-compliance. Delivering high performance and scalable security on NGINX's Application Deliver Controller, enable consistent controls for web apps, microservices, containers, and APIs. Centrally manage and automate approved security controls to remove workflow bottlenecks and support “shift left” dev initiatives.

F5 Silverline provides DDoS, WAF, and fraud prevention with the guidance and care of F5's fully managed services, including global 24x7 support. F5 Silverline detects and mitigates even the largest volumetric DDoS attacks before they ever reach your network. Prevent fraud and degraded customer experiences by detecting bots, fake users, and unauthorized transactions while protecting your web apps and data.

F5 BIG-IQ® Centralized Management provides application-centric visibility and analytics to monitor your applications' health and performance. BIG-IQ Centralized Management offers device, network, security, and application-level visibility and insights with personalized, role-based, per-app dashboards. Give your support teams the data they need to address issues directly from analytics with actionable insights. You can also connect BIG-IQ Centralized Management to upload collected telemetry to your preferred analytics solution to provide insights where your teams are already investigating.

NGINX Controller provides API-driven, cloud-agnostic visibility, no matter where you deploy NGINX Plus. Your analytics scale with your applications, seamlessly integrating and collecting data for up-to-the-minute analysis. All your teams—DevOps, NetOps, SecOps, and AppDev—can collaborate through application-centric monitoring. This ensures everyone gets the information they need, while keeping issues small and manageable.

Automate with Industry-Leading Partners

Learn what many F5 customers already use to deploy securely across their application portfolio. F5 partners with every major cloud provider to ensure our suite of application security and traffic services is available for customers wherever they deploy. F5 works together with industry-leading automation and workload management solutions to build resilient solutions in private, public, and hybrid cloud environments.

aws

ANSIBLE

Microsoft Azure

Google Cloud

HashiCorp

openstack.

Learn more about F5's technology alliances.

Conclusion

F5's portfolio of industry-leading security and application traffic management solutions give enterprises across the world the tools they need to deliver safe and fast applications on any platform—in the cloud or on-premises. Forty-eight of the Fortune 50 rely on F5 to ensure their customers receive a superior and safe digital experience. Scale your applications with F5 and scale your enterprise.

To learn more, contact your F5 representative, or visit F5.com

[1] IDC: The State of IT Resilience Report 2019, found at https://www.zerto.com/page/idc-the-state-of-it-resilience-report-2019/

[2] PricewaterhouseCoopers research report, Experience Is Everything: Here's How to Get It Right, found at https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/pwc-consumer-intelligence-series-customer-experience.pdf#page=8

[3] Salesforce 2018 State of the Connected Customer Report, found at https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/e-books/state-of-the-connected-customer-report-second-edition2018.pdf

[4] Salesforce 2019 State of the Connected Customer Report, found at https://c1.sfdcstatic.com/content/dam/web/en_us/www/assets/pdf/salesforce-state-of-the-connected-customer-report-2019.pdf

[5] Flexera 2020 State of the Cloud Report, found at https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020

©2021 F5, Inc. All rights reserved. F5, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5, Inc.