



F5 and NetApp deliver digital operational resiliency (DOR)

F5 and NetApp help organizations quickly and securely move and store data where and when it's needed to improve data mobility and hybrid multicloud ROI, reduce overhead, and support digital resilience.



0101011
1011010
11011011

Key benefits of F5 and NetApp joint solutions

Enable multicloud

Quickly establish secure and consistent storage and networking for hybrid multicloud environments.

Stay private

Ensure resiliency with highly available, high-speed private connectivity.

Minimize disruption

Centralize observability and diagnostics for improved risk management and faster issue resolution.

Simplify repatriation

Reincorporate workloads back in-house in the event of a cloud failure.

Support compliance

Support DOR and other frameworks to improve resiliency and reduce risk from third-party providers.

Resiliency is more than a strategy, it's often a requirement

Cloud has enabled great scale, efficiency, and innovation, but the shift to cloud services has also created a concentration of dependencies that puts industries and companies at risk in the face of digital disruption, whether from a cyberattack, regional disaster, or service outage. Various digital operational resiliency (DOR) regulations around the world, such as the Digital Operational Resilience Act (DORA) in the EU, set a standard for financial services resiliency in their respective regions. These regulations are not just strictly for financial institutions, they also often apply to third-party service providers, and failure to comply with these standards can result in harsh penalties. As an example, in the EU, organizations that don't comply with DORA, which went into effect January 2025, face a potential penalty of **up to one percent of a company's average daily worldwide turnover**.

Whether your business is accountable to DOR or not, DOR should be a priority to ensure business continuity for any modern, tech-driven company.

Multicloud operational resiliency with F5 and NetApp

Multicloud strategies to avoid cloud concentration are important but also increase complexity with the potential for cloud lock-in and unique networking configurations for each silo.

F5 and NetApp make it possible to quickly and securely move and store data where and when it's needed, improving data mobility and hybrid multicloud ROI, reducing overhead, and bolstering resilience.

F5 secure multicloud networking and global load balancing	NetApp ONTAP (AWS/Azure/GCP)
<ul style="list-style-type: none">• Easily interconnect hyperscale clouds and on-premises sites• Increase security efficacy for traditional and modern apps• Reduce overhead with a unified policy engine and centralized management	<ul style="list-style-type: none">• Optimize cloud storage costs and performance while enhancing data protection, security, and compliance• Simplify native cloud storage and data mobility• Replicate data quickly and easily across zones, regions, and clouds

Key features of F5 and NetApp joint solutions

Facilitate multicloud operations

Support consistent app delivery, security, and networking policies across data centers, cloud, and edge.

Integrate layer 3 security

Safeguard connections with site-to-site VPN and routing, custom network segmentation, and network firewall with egress security.

Simplify operations

Centralize operations for policy configuration and reporting with rich analytics.

Leverage an end-to-end global private network

Connect and secure workloads across multicloud and edge with a purpose-built, private backbone.

Strengthen app security

Enable robust protections with unified, AI- and ML-powered web application and API protection (WAAP).

Improve reporting

Quickly pull summarized logs for audits with Distributed Cloud Console AI assistant.

Data and workload mobility

F5 and NetApp make it easy to quickly and securely move and store data in response to cyber incidents, digital disruption, or other instances of downtime, improving data mobility and resiliency.

Together, F5 and NetApp offer a joint solution that simplifies network routing when you create, replicate, back up, scan, classify, and tier data with NetApp ONTAP. This solution is available on NetApp Cloud Volumes ONTAP (CVO), Amazon FSx for NetApp ONTAP (FSxN), Azure NetApp Files, Google Cloud NetApp Volumes on GCP, and in conjunction with NetApp SnapMirror. F5® Distributed Cloud Services enhances NetApp ONTAP by allowing you to:

- Easily connect to any hyperscale cloud, sovereign cloud, or on-premises site
- Reduce complexity and overhead for IT
- Tap into the security and high performance of the private F5® Global Network

All workloads are visible and controlled from the F5® Distributed Cloud Console, with the ability to enforce data security requirements using additional cyber-resilience tools, as required by many regulatory compliance frameworks, including DORA.

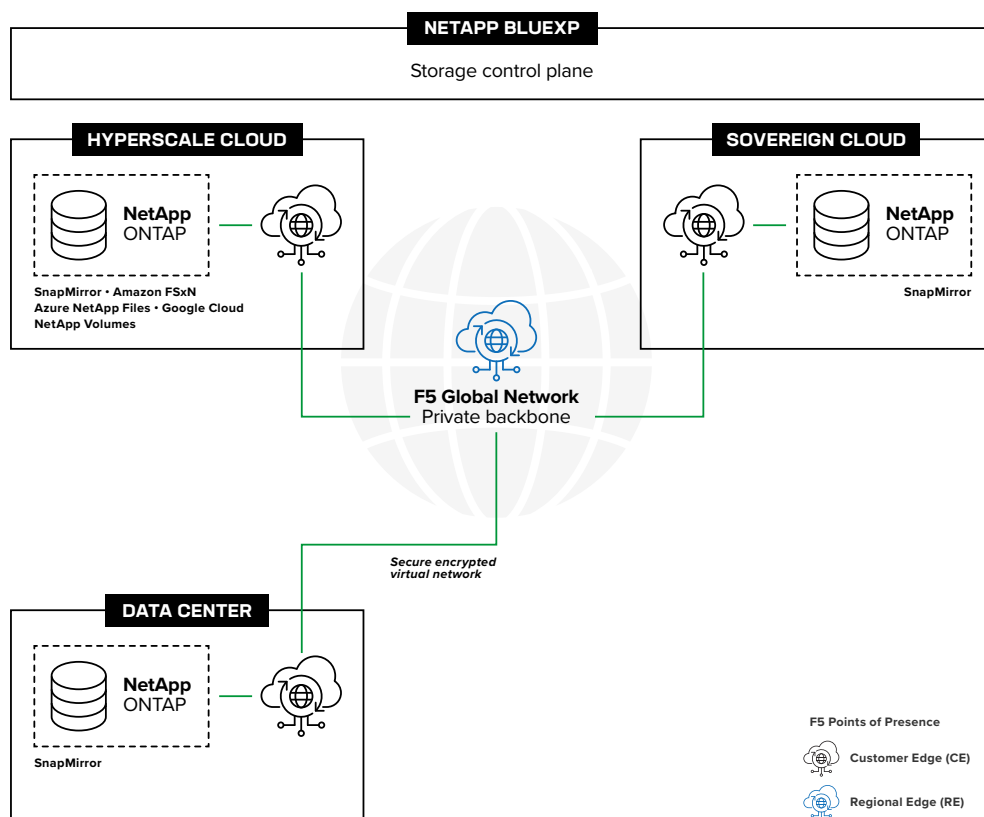


Figure 1: Secure data migration and replication with F5 and NetApp.

Geo-redundancy and secure data delivery

NetApp StorageGRID, a software-defined object storage solution for hybrid multicloud environments, supports digital resiliency by providing a robust, secure platform for managing vast amounts of unstructured data with high availability, integrity, and confidentiality.

F5 enhances StorageGRID deployments with geo-redundancy and secure data delivery for HTTPS servers via the S3 protocol, improving real-time operational resilience in the event of cloud provider or data center disruptions.

F5® BIG-IP® DNS delivers global server load balancing (GSLB) for intelligent routing across multiple StorageGRID sites. This functionality ensures smart routing to the closest destination site within the namespace, and includes outage detection with automatic redirection to the next available site. A high-availability (HA) implementation includes a top-level GSLB setup with site pools containing F5® BIG-IP® Local Traffic Manager™ (LTM) for site-level load balancing.

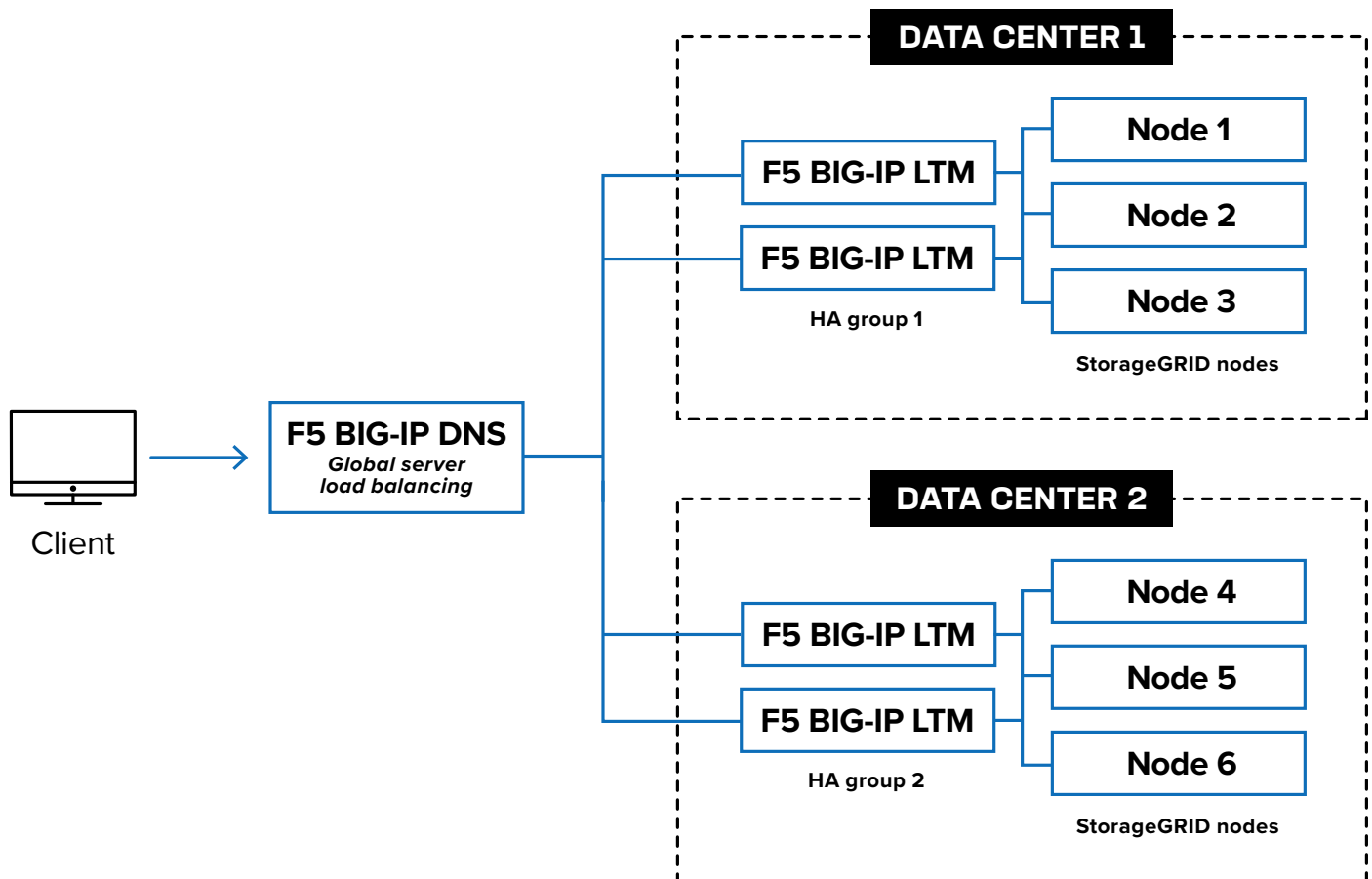


Figure 2: Global and local traffic management for NetApp StorageGRID with F5® BIG-IP®.

Enhanced DOR with traffic protections and automated scanning

In addition to enhancing NetApp ONTAP implementations, F5 Distributed Cloud Services offers several standalone capabilities that enable greater control over traffic management to protect your digital landscape. Features such as managed layer 3 distributed denial-of-service (DDoS) protection, rate limiting, and region- or geography-based traffic blocking help keep your organization's web services responsive. Distributed Cloud Services can also automatically ignore or send HTTP 427 status codes to impede a discernible source that's sending a flood of requests.

To comply with DOR requirements, many enterprises need to prove they are testing their web services proactively and frequently. Teams can use F5® Distributed Cloud Web App Scanning for automated reconnaissance and penetration testing. Accessible through the Distributed Cloud Console, this service scans for vulnerabilities in web applications, provides recommendations for web application firewall (WAF) rules, and suggests other remediations to mitigate security risks effectively.

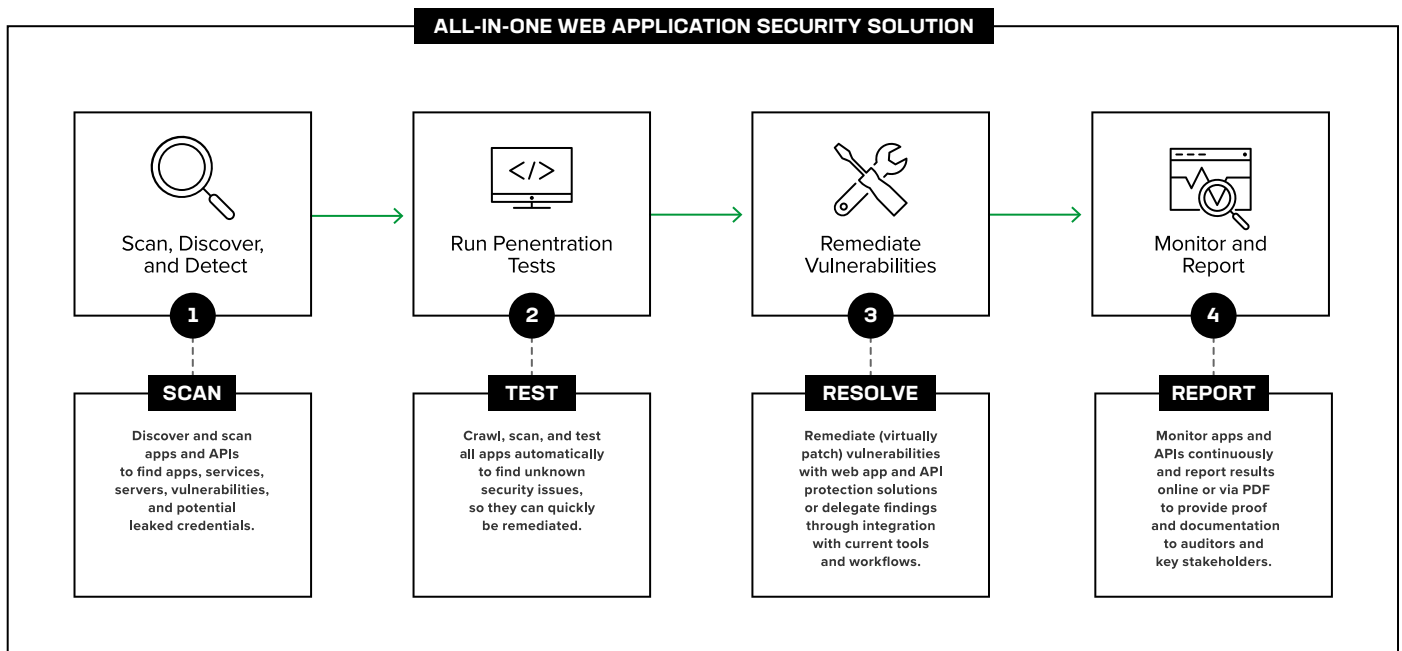


Figure 3: Automate penetration testing and get recommendations to keep your environment secure.

Multicloud application security with F5

Digitally driven companies need to implement advanced cybersecurity measures, such as real-time threat detection and automated incident response systems, to safeguard customer data and maintain service continuity during cyberattacks or outages.

F5 allows organizations to connect, protect, and deploy apps seamlessly across distributed clouds, supporting hybrid multicloud strategies needed for DOR and compliance with various security frameworks. With F5® Distributed Cloud Web Application and API Protection (WAAP), organizations can accelerate time-to-service, reduce total cost of ownership, and increase security efficacy. This solution is built on a cloud-native platform fully integrated with a single policy engine and a unified management console for streamlined operations.

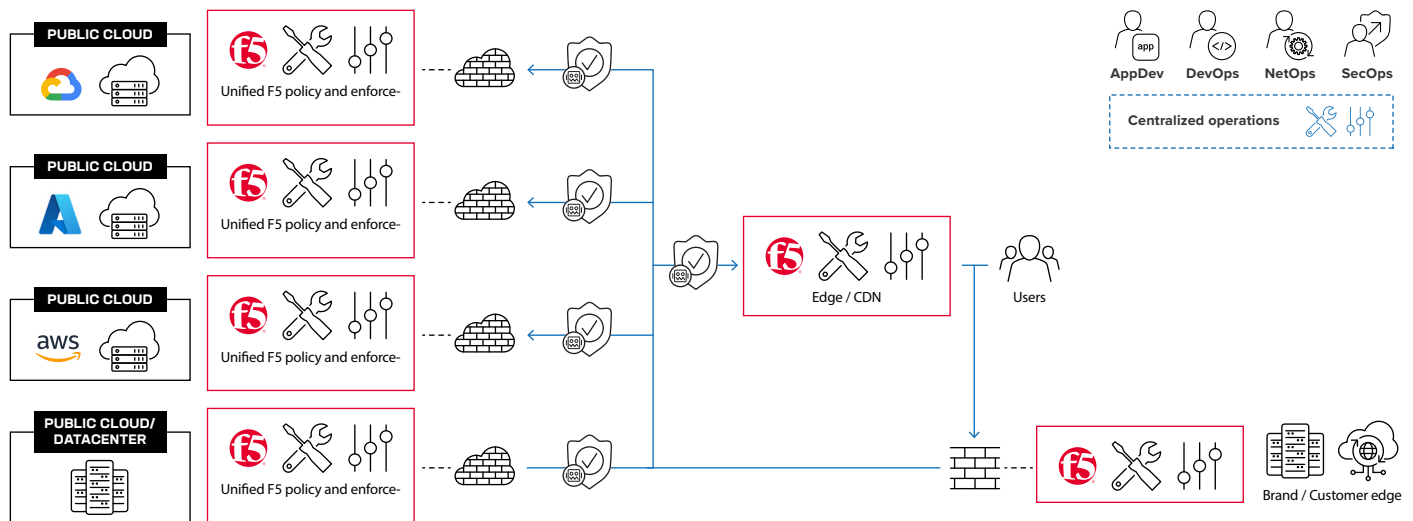








Figure 4: Unified policy management and enforcement with Distributed Cloud Services.

Key WAAP defenses and capabilities include:

Web application firewall	 Signature-based identification	 Behavior-based identification of threat actors and false positives
DDoS mitigation	 Volumetric network layer (L4) DDoS	 Application layer (L7) DDoS
Bot defense	 Bot detection and mitigation Identify automated, non-human attacks that can flood digital infrastructures	
API protection	 API discovery and security Easily identify all API endpoints mapped to applications and anomalous activities	

F5 and NetApp improve your digital operational resilience

F5 and NetApp offer integrated solutions featuring advanced DDoS mitigation, intelligent bot detection, and comprehensive API protection to enhance cybersecurity and performance. Key products like StorageGRID, BIG-IP, and Distributed Cloud Services provide secure data storage, smart traffic management, and cloud-based security. BIG-IP further enhances operational resilience by delivering intelligent load balancing for S3 workloads, efficiently distributing traffic across storage endpoints to ensure high availability, scalability, and optimal performance. These solutions help block automated attacks, monitor API usage, and ensure resilient operations.

Learn how F5 and NetApp can strengthen your digital defense at f5.com/netapp.

