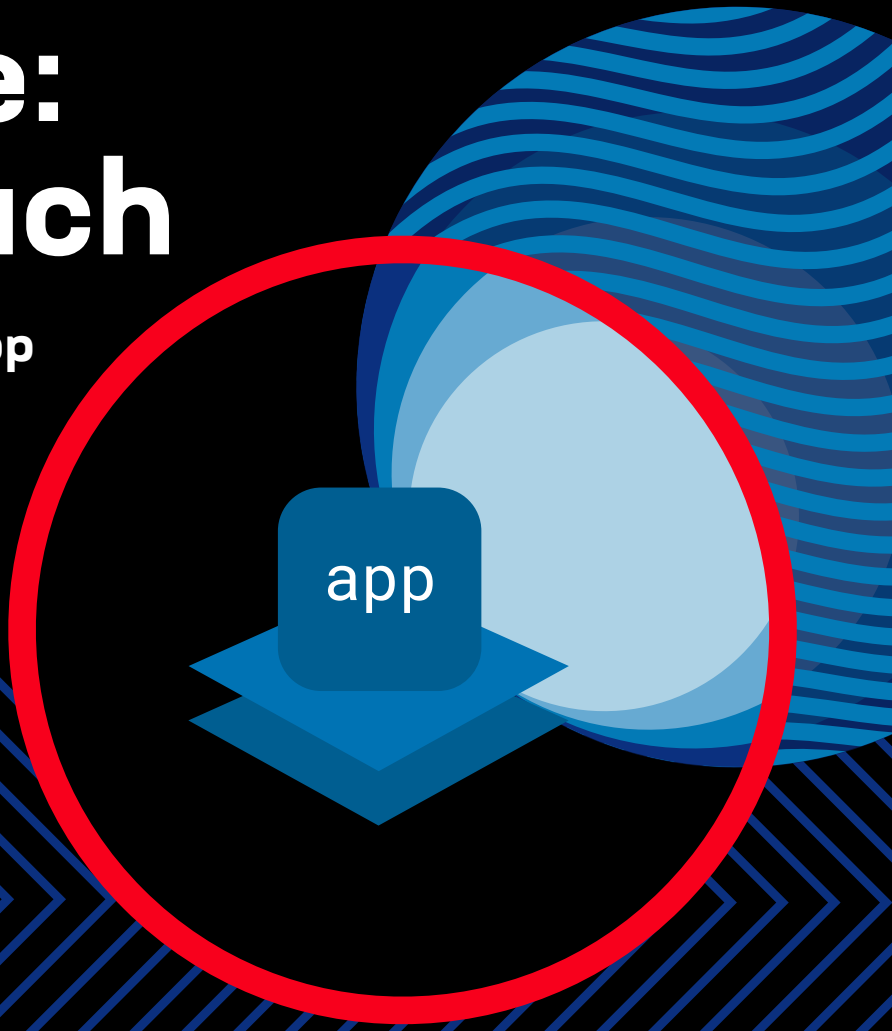
Unify and protect your digital estate: a platform approach

A practical path to deliver and secure every app and API in any environment



Contents

Who needs this eBook

Financial leaders

Recognize the cost benefits of consolidating tools and vendors using an app delivery and security platform approach.

Security leaders

See how platform-based API lifecycle protection, bot and DDoS defenses, and identity-aware controls deliver consistent policy enforcement across clouds, data centers, and the edge.

Networking teams

Appreciate how the platform approach provides the any-to-any traffic management, globally resilient network and DNS performance, multicloud networking, and form-factor flexibility to meet apps where they run without rearchitecture work.

Platform teams

Learn how standardizing and streamlining core components of infrastructure can improve reliability and security while enabling automated development pipelines and streamlining innovation.

Developers

Understand the platform guardrails and integrations needed to deploy faster and with more confidence.

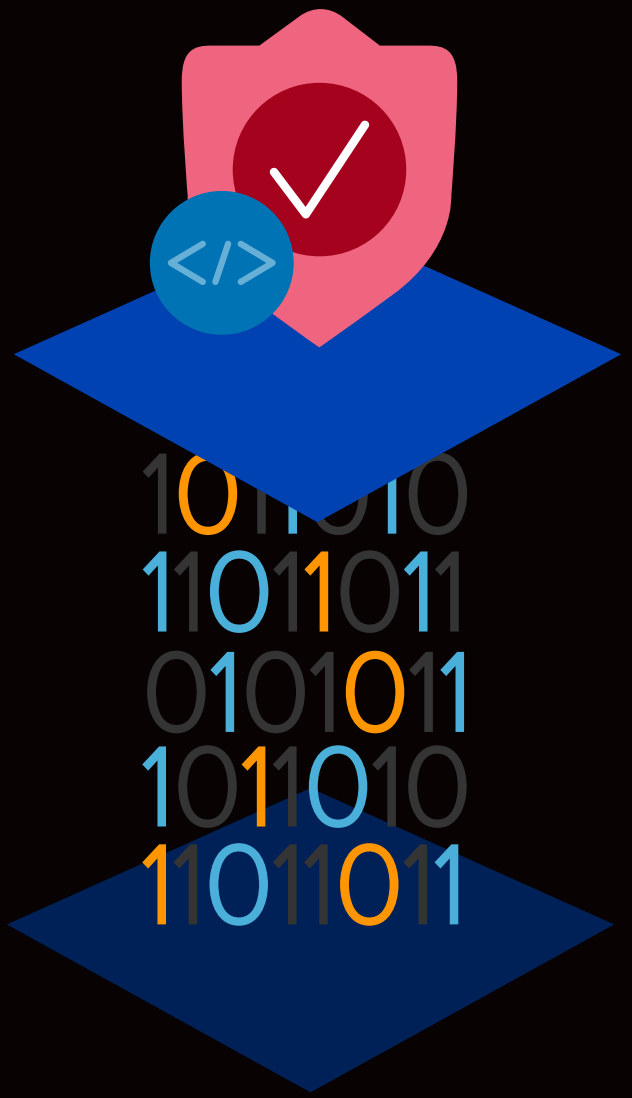
Executive summary

Digital experiences are the front door for customers across every industry. Whether stepping through that door entails a banking transaction, a citizen request for government services, provisioning a workflow, or a checkout flow during a seasonal sales spike, users expect instant, reliable, and secure interactions. Behind the scenes, those experiences are powered by applications and APIs that are no longer hosted in a single place. They span data centers, multiple public clouds, edge locations, and an expanding constellation of AI workloads that create new data paths, threats, and performance requirements. This distribution brings freedom, performance gains, and agility to the organization—but it also introduces risk, operational drag, and a growing gap between how fast you need to move and how fast your tools let you move.

Most teams have addressed these challenges with point solutions. These frequently include one tool for web app security, another for API protection, separate systems for DNS and traffic management, more for DDoS mitigation, and still others for bot defense, access security, app and traffic visibility, and automation. Each tool can be effective on its own, but together they create operational complexity: overlapping products, inconsistent policies, and blind spots that attackers exploit. The result is higher costs, disruptive change management, and security postures that vary by environment.

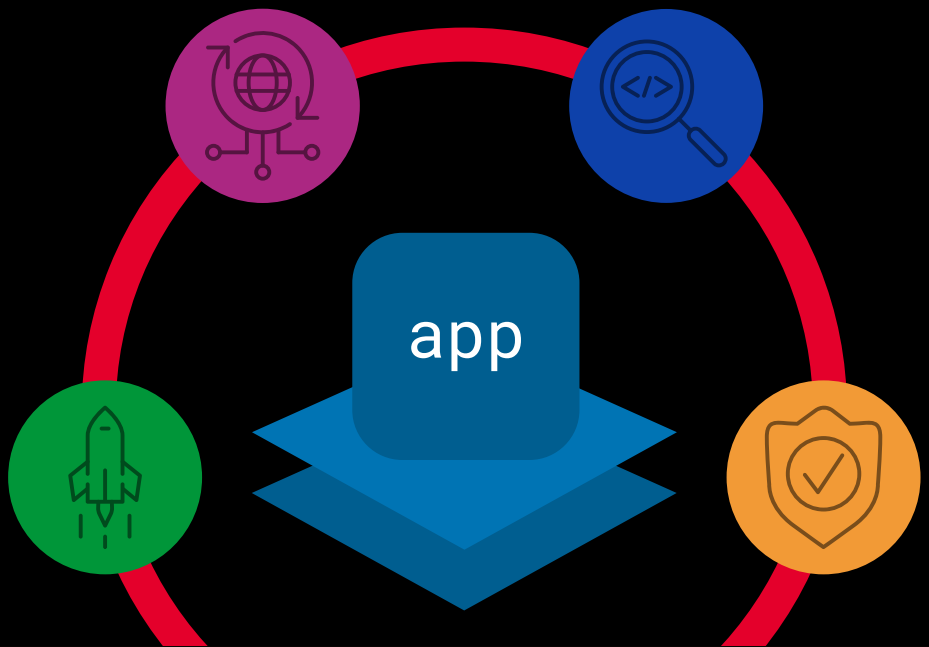
There is a better way. A platform approach converges app delivery and security so you can manage every app and API in distributed environments with unified visibility, automation, and AI-driven insights. Key considerations for a platform approach include:

- Instead of handcrafting integrations across products and clouds, standardize policies and workflows once and propagate them everywhere.
- Instead of manually correlating telemetry from multiple consoles, access actionable insights (not just raw stats) that connect status detection to responses.
- Instead of choosing between performance and protection, optimize for both.



That's the promise of a converged platform approach. This eBook shows you how a platform-centric strategy helps address the challenges of hybrid multicloud environments in the AI era. Keep reading to:

- **Reflect on how the game has evolved** with hybrid multicloud and AI environments—including why preexisting platform categories (such as XDR, SASE, CNAPP, and others) can't fully solve the resulting app and API challenges.
- **Explore what "good" looks like** for global application delivery, how modern security must be embedded end-to-end, and why operational simplicity is the real force multiplier—including its impact on developer and business agility.
- **Learn about the F5® Application Delivery and Security Platform (ADSP)**: a single, converged platform that unifies app delivery and security with portfolio-wide visibility and automation.
- **Consider F5 ADSP benefits**—including application performance and availability, AI-driven insights, unified observability, and operational simplicity.
- **See how these benefits translate into measurable outcomes**. Read stories from other organizations that have already adopted a platform approach and consider relevant key performance indicators (KPIs) for your own executives, which might include:
  - CISO: Reduce risk exposure and mean time to respond, increase the percentage of APIs discovered and protected, and improve audit readiness with centralized evidence.
  - CIO: Enhance availability and latency service level agreements (SLAs) across environments, expand automation coverage, and reduce tool and vendor count to lower operational drag.
  - CFO: Reduce costs-to-serve and incident impact, drive predictable TCO through consolidation and standardization, and minimize spend on bespoke integrations.
- **Identify next steps** for your organization.



The Ball of Fire: sprawl, scale, and exposure

A decade ago, most apps lived in a handful of data centers. Today, critical services span on-premises infrastructure, multiple public clouds, edge locations, and partner ecosystems. Legacy systems and apps coexist with microservices, serverless components, and AI models that demand high throughput and low latency. The distribution of multigenerational apps and components increases agility—but it also multiplies the opportunities for things to break, the surfaces where attackers can probe, and the operational seams where policies and accountability get fuzzy.

F5 calls this complexity—and the accompanying risks—the "Ball of Fire," and most organizations today feel the burn.

The distribution of multigenerational apps and components increases agility–but it also multiplies the opportunities for things to break.

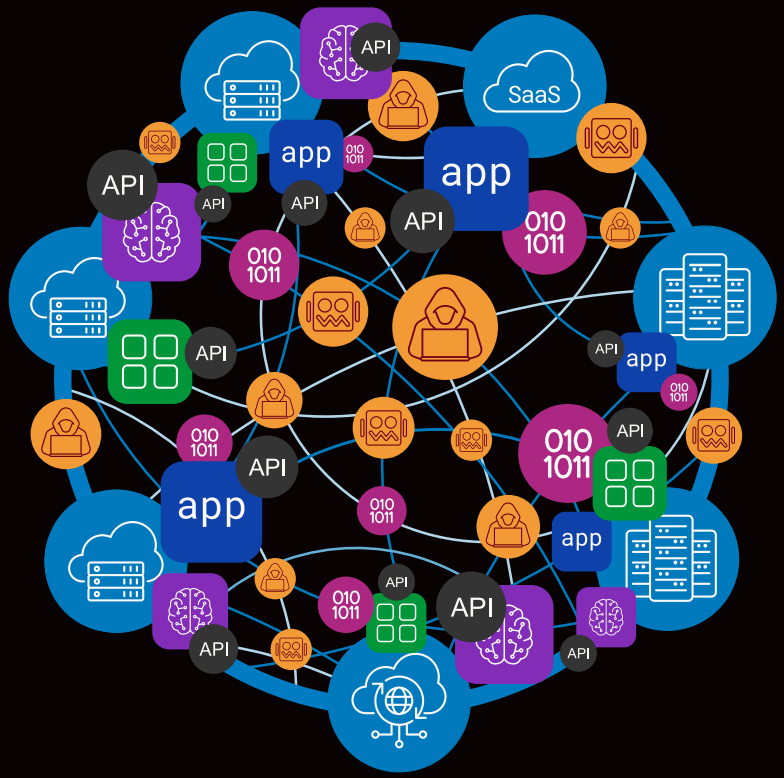


Figure 1: The Ball of Fire resulting from today's hybrid, multigenerational, multicloud application and API deployment landscape.

How we got here

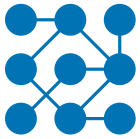
A variety of trends have contributed to infrastructure complexity, resulting in the Ball of Fire:

Distributed infrastructures as the default

The advantages of hybrid multicloud deployments have made them the norm. Very few organizations today deploy apps and APIs in a single cloud. In fact, F5 research summarized in the F5 2025 State of Application Strategy Report suggests that 94% of organizations distribute apps across multiple deployment locations or models to gain flexibility and cost savings. As a result, most organizations operate mixed environments, often with regulated workloads on-premises, latency-sensitive services at the edge, and elastic components in one or more public clouds. Such distribution is logical, but it fragments app delivery and security.

Attacker evolution

AI-powered attacks accelerate reconnaissance and the creation of exploits, fuel "human-like" bot swarms, and enable polymorphic attacks. Business logic, identity flows, and fast-changing or shadow APIs are prime targets, while DDoS campaigns blend volumetric surges with precise layer 7 tactics. AI-native threats (such as prompt injection, jailbreaks, model poisoning, and model exfiltration) are rapidly expanding the attack surface and compressing response windows.



APIs everywhere

APIs power mobile apps, partner integrations, and internal microservices. They accumulate fast and change frequently. As a result, organizations end up dealing with shadow APIs, stale versions, and inconsistent enforcement—prime targets for attackers and a source of audit pain.

Operational constraints

The human layer doesn't readily scale. If different environments require different consoles, policies, and playbooks, even top teams end up chasing configuration drift. Manual handoffs introduce delays. "Eyes on glass" monitoring without guided remediation overwhelms analysts and engineers. The cost is real: incidents last longer, change windows shrink, and talent burns out.

Where current approaches fall short

Over the past few years, several platform categories and point solutions have sought to address elements of the Ball of Fire. These solutions add value to app and API delivery and protection, but they don't address the challenges holistically. Specifically:

- **Secure access service edge (SASE) solutions** deliver powerful access and edge security, applying zero trust security to users and devices. But SASE isn't a replacement for global application delivery, multicloud traffic engineering, or deep API protection. It governs who connects, but it doesn't ensure the app is resilient and defended throughout its lifecycle.
- **Cloud-native application protection platforms (CNAPPs)** offer a strong build-time and cloud runtime posture via tools such as Kubernetes security, infrastructure as code (IaC) scanning, cloud security posture management (CSPM), and cloud workload protection (CWPP). However, CNAPP typically stops short of unifying delivery, multicloud networking (MCN), and layer 7 runtime controls for all apps, including those outside a specific cloud. CNAPP is necessary but not sufficient when your estate spans clouds, data centers, and the edge.
- **Endpoint protection platforms (EPPs)** secure devices and improve device security postures to prevent and contain threats on endpoints (such as malware, ransomware, and other exploits). But EPPs don't deliver applications, enforce runtime API policies, mitigate bot or layer 7 DDoS attacks, orchestrate cross-cloud traffic, or unify delivery and protection for distributed apps and APIs.
- **Extended detection and response (XDR) solutions** are excellent for correlating endpoint and security telemetry and speeding incident response. But XDR isn't designed to deliver applications, enforce runtime API policies, or orchestrate cross-cloud traffic. Without integrated layer 7 controls and delivery context, XDR solutions can see symptoms without being able to act on root cause patterns in the app pathway.
- **Hybrid, multicloud frameworks (HMF)** connect infrastructures and normalize overlays across clouds. Where they fall short is the application layer: unified security, AI-driven intelligence, and full-stack observability tied to dynamic traffic flows. An HMF often connects networks, but it rarely connects app delivery and protection as a single function.
- **Enterprise data protection (EDP) solutions** are critical for encryption, key management, and data loss prevention (DLP). But EDP focuses on data as an object. It generally doesn't control the application and API pathways to provide traffic management, bot and DDoS defenses, or policy orchestration across environments.
- **Identity and access management (IAM)** provides the backbone for single sign-on (SSO) access and authorization, including multifactor authentication (MFA). Yet identity context is rarely enforced uniformly at layer 7 or the data plane across hybrid multicloud environments. IAM does not provide runtime API, bot, or DDoS protection or deliver apps with the resilience users expect.

Taken together, these platform categories and solutions form a strong ecosystem, but they fail to converge application delivery and security into one unified fabric with shared policy, telemetry, and automation. That missing convergence is the source of many operational challenges: duplicated controls, drift between environments, and gaps at the exact moment applications need to scale or defend themselves.

By contrast, operational simplicity is a multiplier that benefits app development and business agility. Achieving this simplicity requires app delivery, security, and telemetry services that operate together, driven by shared visibility and policy enforcement, across distributed environments.

Challenges by industry

Financial services and fintech

Digital and open banking, payments, and trading platforms are API-heavy and latency-sensitive, with constant fraud and bot pressure. Although regulatory scrutiny demands provable controls and fast audits, tool sprawl complicates risk management and increases costs.

Healthcare

Patient portals, EMRs, and telehealth require strong security for protected health information (PHI), zero tolerance for downtime, and auditable controls across hybrid estates.

Manufacturing

OT/IT convergence increases the use of edge sites and supplier APIs, while low-latency control loops and site-to-cloud paths need reliability and protection without adding overhead.

Retail and e-commerce

In a hypercompetitive market, any glitch, delay, or security issue drives customers away—hurting conversion, revenue, and brand loyalty. Seasonal traffic spikes may compress traffic and revenue into short bursts in which bots target the business logic supporting inventory, pricing, and checkout processes.

Public sector and education

Lean teams work under significant budget constraints to operate legacy systems alongside modern cloud services, struggling to keep policies consistent across environments while meeting strict regulatory requirements and maintaining clear evidence for audits. DDoS and the risks of account takeover spike during elections, enrollment, and similar major events.

Technology

Teams need repeatable, standardized workflows and guardrails that don't slow delivery to environments that are multicloud by design, with rapid release cycles and microservice architectures. AI models and data pipelines add throughput and security requirements. Plus, as AI deployments evolve, XOps needs support to defragment voluminous telemetry and convert it into insights, actions, and process standardizations.

Telecommunications

S/Gi firewall needs, regional policy enforcement, and edge delivery create a unique blend of performance and protection requirements that must stay consistent through massive scale and global footprints.

Simplify the Ball of Fire with unified app delivery

Users don't experience your network, clouds, or security tools. They experience your applications, and they don't negotiate with latency. If a login stalls, a stream buffers, or a checkout lags, they abandon.

Meeting user expectations requires standardized blueprints that keep applications close and data flowing while remaining resilient to failures and surges. But what does "good" app delivery look like today? When apps span data centers, multiple public clouds, and edge sites, the definition of "good" includes high app availability, speed, resilience, security, and deployment agility. To achieve those performance measures, teams tasked with app delivery require unified tools that adhere to five principles: reach, intelligence, resilience, efficiency, and neutrality to underlying environments.

Five principles of unified app delivery

1. Reach: Provide any-to-any delivery across regions, clouds, and the edge

Global footprints are now table stakes. Traffic should be directed to the nearest healthy endpoint or storage module across data centers and multiple clouds, with smart geographic and network-aware routing. Edge locations can terminate connections, cache, or preprocess data to reduce round trips and keep user interactions efficient. Your delivery fabric must span everywhere your apps are hosted and wherever your users may be, regardless of geography or environment, without bespoke engineering per location.

2. Intelligence: Steer by signal, not guesswork

Modern app delivery uses dynamic signals—real-time health checks, latency, saturation, and business context—to make decisions. That means you need:

- Layer 4–7 load balancing across clusters and regions using live telemetry
- Traffic engineering that adapts to ISP congestion, cloud regional incidents, and application saturation
- API-aware routing that understands versioning, headers, and methods, not just IPs and ports
- Demand shaping (rate limits, QoS, and prioritization) to preserve critical flows during spikes

3. Resilience: Design for failure and fast recovery

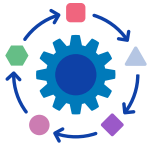
Assume zones, links, and services will fail, but deploy these proven practices to help avoid outages and risks:

- Authoritative, resilient DNS with short TTLs and automated failover
- Health-driven routing and circuit breakers to isolate unhealthy endpoints
- Blue/green and canary patterns to shift traffic safely during releases
- Disaster recovery that leverages secondary regions with prewarmed capacity, not just cold backups

4. Efficiency: Ensure performance without wasted resources

Performance and cost aren't enemies. Techniques to simultaneously deliver both include:

- Faster data delivery via a content delivery network (CDN) and object caching with precise cache control
- Connection multiplexing and TLS optimization to conserve CPU utilization
- Hardware-accelerated data paths and hardware acceleration for encryption and compression when volumes climb
- Programmable data planes to push policy enforcement closer to where traffic flows



5. Ubiquity: Meet the app where it runs

Form factors matter in hybrid and multicloud environments, and app delivery controls should operate consistently across:

- Kubernetes clusters (ingress/egress), including multi-cluster and multi-cloud topologies
- Virtualized or software instances in public and private clouds
- Edge and branch locations with constrained resources
- Hardware in high-throughput or regulated environments
- As-a-Service models for rapid rollout and centralized governance

CUSTOMER SUCCESS

Performance and resilience

An investment management company facing risks to operational continuity partnered with F5 to upgrade its hybrid app delivery and security infrastructure by unifying disparate tools across on-premises and cloud environments. F5 ADSP enabled the company to increase overall app resiliency, add redundancy to protect service availability, and optimize performance within existing budgets.

Integrate security for end-to-end protection

Cyberattacks follow the path of lowest cost and highest return, and today that path often flows through the application and API layer. Successful defenders win by moving security into the delivery path and making protection continuous across the app and API lifecycle—from discovery, assessment, and enforcement to observation and adaptation.

CUSTOMER SUCCESS

Security and compliance

A major F5 banking customer modernized its architecture and operations across its hybrid data center and multicloud environments. In addition to supporting the company's shift to containerization, F5 ADSP remediated critical gaps in API and DNS security. Converging app delivery and security allowed the company to enhance scalability across hybrid multicloud environments while increasing resilience for 24/7 service, improving disaster recovery capabilities, and facilitating regulatory compliance.

Eight principles of unified security

The following eight principles enable secure, integrated, and reliable app delivery.

1. Prioritize visibility: you can't protect what you can't see

Continuously discover, inventory, and classify applications, their components (such as front ends, microservices, data stores, and LLM/inference endpoints), and all APIs. Map dependencies and data flows across regions/clouds; model baseline behavior to detect anomalies. This mapping helps you to connect each asset to an owner, business priority, data classification, and risk posture.

2. WAAP as a fabric, not a function

Web app and API protection (WAAP) should act like a distributed fabric, enforcing the same controls everywhere traffic enters.
Core capabilities include:

- Intelligent web application firewall (WAF) services that understand application behavior and blocks exploits while minimizing false positives
- Bot management that distinguishes automation from human users and protects sensitive data and business logic such as login, account changes, or checkout processes
- DDoS mitigation at network and application layers that scales with surges while absorbing or deflecting attacks without human intervention
- API protection that enforces schemas and behavior, rate limits and quotas, and context-aware policies (such as client, identity, or geography policies)

3. Identity-first, zero trust security

Identity is the new perimeter—but only if enforced consistently. Practical zero trust security for apps includes:

- Strong authentication and adaptive access (SSO/MFA) with continuous verification
- Micro-segmentation of applications and APIs by purpose and sensitivity while applying least privilege principles for users, services, and machine identities
- Enforcing identity propagation at layer 7 so decisions travel with each request across clouds, clusters, and environments
- Policy-based visibility and traceability into encrypted traffic (such as TLS/HTTPS) with selective decryption, privacy controls, and full auditability

4. High-performance firewalling with behavioral and threat intelligence

Network controls still matter—especially in hybrid environments and service provider contexts. A firewall that understands applications (not just ports) helps to prevent lateral movement, contains volumetric floods, and enforces policies where network boundaries still exist. Pairing these controls with delivery telemetry produces smarter decisions and faster automated responses.

Eight principles of unified security (Cont.)

5. Threat intelligence that adapts in real-time

Static lists and weekly reports can't keep pace. Security improves when enforcement points consume adaptive intelligence about reputations, exploit campaigns, bot signatures, and anomaly patterns learned across environments. The result is faster suppression of known bad clients and earlier detection of emerging attack techniques.

6. Protection for AI models, prompts, and data

LLM-enabled apps introduce new risks, including prompt injection, data leakage, model abuse, evasion attacks, and sensitive output. Practical safeguards include:

- Inspection and sanitization of prompts and responses
- Policy guardrails to prevent exfiltration and disallowed outputs
- Redaction and masking for sensitive data
- Granular observability of model latency, token usage, and anomalies to help teams balance accuracy, cost, and risk

7. Encryption at scale without blind spots

Organizations need privacy-focused strategies to inspect traffic, permitting only authorized users, orchestrating TLS/SSL efficiently, and ensuring readiness for post-quantum cryptographic algorithms. Centralizing certificate lifecycle management and offloading cryptographic processes in high-throughput paths prevent avoidable outages and conserve CPU power.

8. Shifting people and processes from alerts to actions

Security embedded in app delivery can also respond by blocking threatening traffic, raising friction for suspicious clients, and deflecting floods—automatically—while surfacing concise insights to analysts. This type of embedded security can help you turn telemetry into expedited decision making.

Cyberattacks follow the path of lowest cost and highest return, and today that path often leads through the application and API layer.

Key security concerns by industry

Financial services and fintech

Protect against malicious bots that can result in account takeover, discover and automatically protect APIs associated with growing open finance ecosystems, and quickly access evidence for regulatory audits.

Healthcare

Meet HIPAA, HITECH, PCI DSS, and regional compliance mandates, keep patient portals available, and mitigate increasingly sophisticated ransomware that uses vulnerability exploits, compromised credentials, and infostealer malware to breach protected health information (PHI) or scrape intellectual property.

Manufacturing

Secure all your digital touchpoints, from partner API connections to factory floor operations, to stop threats from spreading.

Retail and e-commerce

Protect critical business logic, including inventory and cart processes, from automated attacks and enforce API governance for partners.

Public sector and education

Stop DDoS attacks during high-visibility events, ensure service availability, and streamline compliance reporting.

Technology

Prevent data breaches and customer account takeover, protect microservices and CI/CD exposure, secure and monitor AI model and inference endpoints, and comply with regulatory requirements such as PCI DSS and General Data Protection Regulation (GDPR).

Telecommunications

Combine high-performance firewalling with layer 7 protections at scale.

How a platform approach can unify app delivery, security, and telemetry

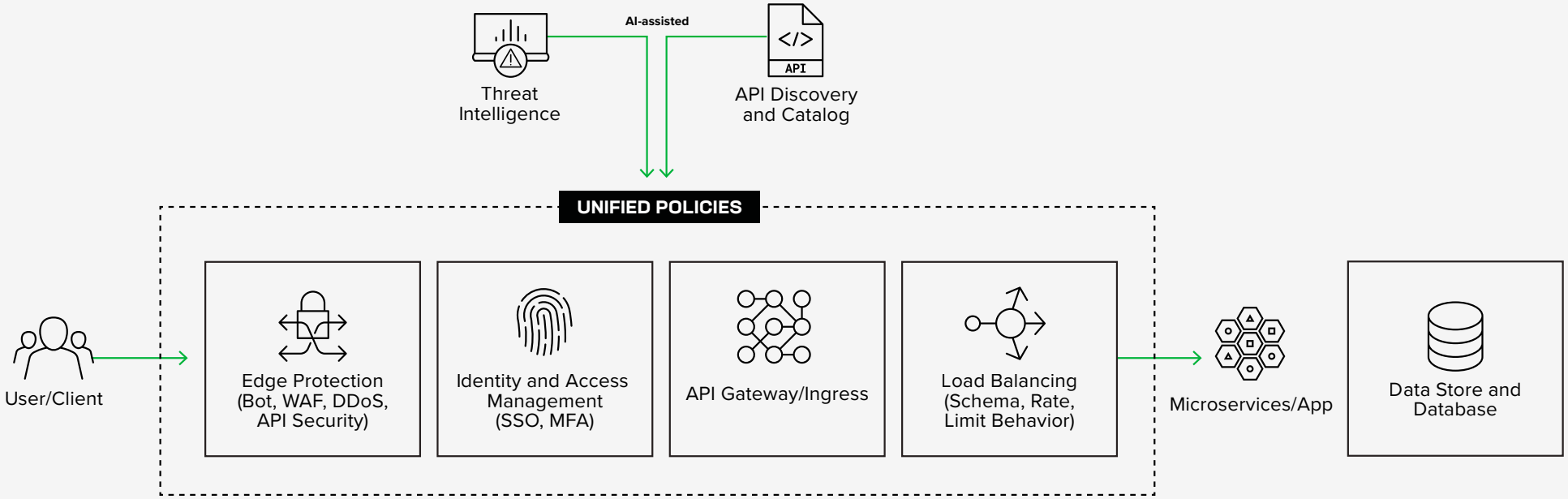


Figure 2: Integrated security and app delivery services provide end-to-end protection and a single pane of glass across deployment environments.

CUSTOMER SUCCESS

Greater application scalability and cost flexibility

A technology company known for its digital human resources and payroll solutions worked with F5 to optimize its app delivery infrastructure across its hybrid cloud and AI environments. By deploying F5 ADSP and leveraging cloud-first solutions, the company gained flexibility in balancing its capital expenditures against operating expenses. By converging app delivery and security, the company also increased scalability, providing support for additional Kubernetes clusters and workloads that enabled rapid expansion to support a key AI project.

Standardize and streamline operations

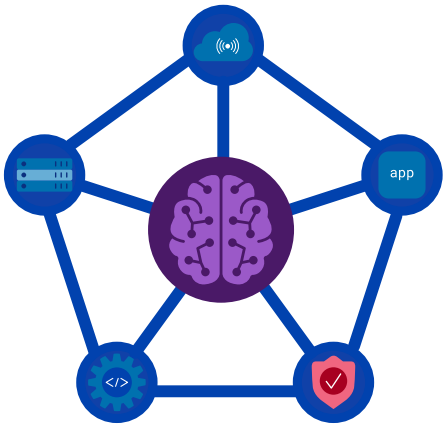
Operational wins come from standardizing how teams see, decide, and act in response to app delivery and security flows, no matter where the apps run.

A single operational plane (even if components are distributed)

Teams need one place to answer four questions:

1. What's running?
2. How is it performing?
3. What's at risk?
4. What's changed?

Unifying related metrics enables operators to correlate symptoms to root causes without moving between consoles. Actionable and context-based telemetry, a reduction in attack surfaces, and streamlined costs are achieved with these five capabilities.



1. Automation that respects guardrails

A scalable, AI-centric approach requires:

- API-first control surfaces
- Policy as code, GitOps practices, and templates (so changes are reproducible)
- Progressive delivery strategies (such as canary or blue/green deployments)

2. Consistent UX and shared workflows

A common experience and standard objects across environments reduce operator error and training requirements. As a result, once complex, hybrid multicloud operations become faster and easier.

3. AI assistance

Natural language assistants can offload labor, generate reports, suggest policies, propose remediations, and shorten the path from signal to action.

4. Governance that proves control

Operational simplicity makes it easier to compile comprehensive evidence for compliance, making audits easier and less resource intensive.

5. Metrics that matter

Operations and reporting become simpler when the platform metrics include not only availability and latency but mean time to resolution (MTTR) for issues, percentages of APIs discovered and governed, percentage of automation, and rate of policy reuse.

A single operational plane to see, decide, and act across all environments

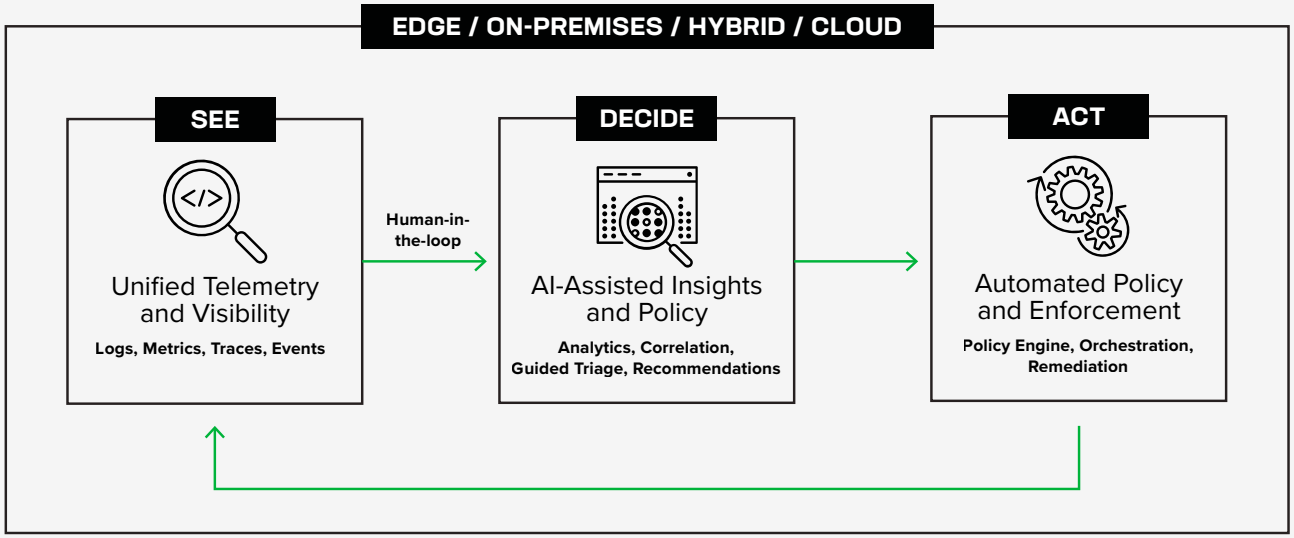


Figure 3: A platform approach can centralize telemetry and intelligence across deployment environments to reduce the labor required for—and speed—tracking, reporting, audits, and other management and governance tasks.

Increase developer and business agility

To innovate at the pace of business in the AI era, developers need fast, paved paths to production while governance and security are encoded as defaults. Drive business agility by delivering these four capabilities:

1. Paved development paths, embedded security, and self-service

Save developer time with standardized blueprints and self-service for ingress, API gateway, and routing needs. Reduce errors with blue/green and canary deployment templates that include built-in metrics and one-click rollback. Erect guardrails for configurations such as rate limits and access policies in effect by default. Deploy shift left and shield right security, both embedded into the CI/CD pipeline and enforcing runtime protections where traffic flows.

2. Service mesh and platform engineering alignment

As organizations adopt microservices, service meshes add observability and enable mutual TLS (mTLS). The delivery and security plane should integrate cleanly, producing one view of services across delivery, security, and mesh management.

3. AI enablement

Scaling AI requires optimizing data ingress and egress for training pipelines. It demands dynamic policy enforcement and intelligent inference traffic routing to protect intellectual property and privacy.

4. Accelerated compliance management

Automating collection of compliance evidence reduces audit cycles. With standard, approved patterns, governance processes can define paths rather than inspect every variation, freeing resources for innovation.

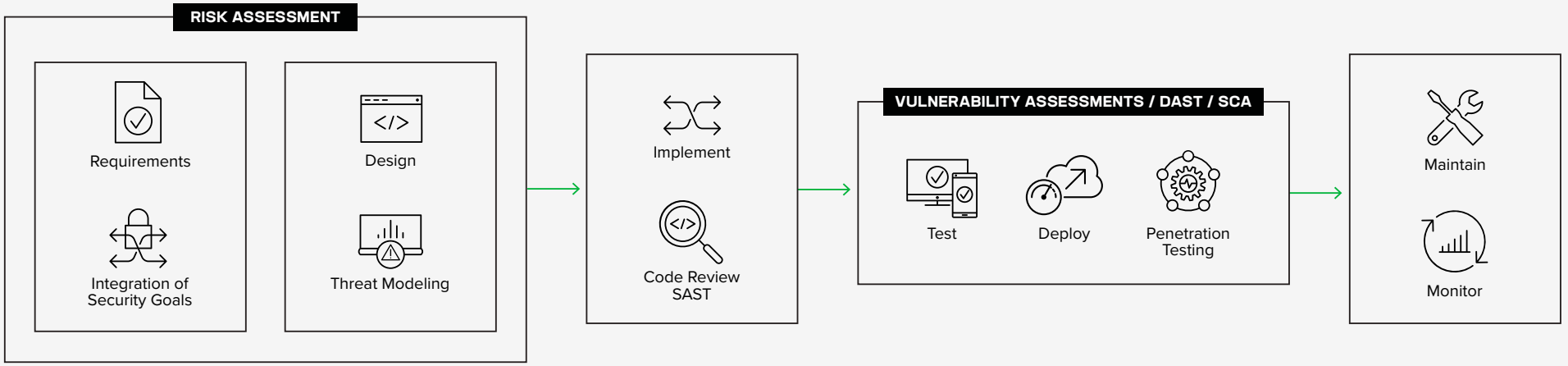


Figure 4: Save developer time while ensuring faster, more secure deployments with a platform approach that embeds security; aligns delivery, security, and compliance requirements; and enables use of AI.

Converge app delivery and security with F5 ADSP

Today's enterprises need a unified way to deliver and protect applications and APIs across data centers, multiple public clouds, and the edge, without trading performance for security or sacrificing speed for governance. F5 Application Delivery and Security Platform (ADSP) converges F5 products to deliver holistic solutions for the AI era. F5 ADSP unifies application delivery and security into a programmable platform, adds portfolio-wide visibility and AI assistance, and keeps policies consistent wherever apps run. The result is a simpler, more secure, faster operating model for every team that manages digital experiences.

Why now?

The ongoing shifts to hybrid multicloud environments and AI-powered initiatives are accelerating at an exponential pace. The F5 2025 State of Application Strategy Report found that:

- 94% of organizations already distribute apps across multiple deployment locations or models
- Although app portfolios are rapidly modernizing, some 15% of the average portfolio will likely remain in legacy apps through the end of this decade
- Nine out of 10 organizations will be using AI-driven automation in their IT operations by 2035

Amid Ball of Fire complexity that is exacerbated by the evolution of AI, IT teams need a single platform that treats app delivery and security holistically. A converged app delivery and security platform provides increased app and API visibility while automating resource-constraining operational tasks.

F5 ADSP brings these capabilities together so you can meet ever-evolving customer expectations, improve security outcomes, and simplify operations—no matter where your apps and APIs run.

Why F5 is uniquely qualified to deliver a unified platform

F5 provides a platform-centric approach that helps organizations deliver and secure every app and API across any environment. For decades, F5 has been a leader in application delivery, keeping digital experiences fast and available for mission-critical services worldwide.

With more than 23,000 customers in 170 countries, F5 delivers and secures apps for more than 80% of the Fortune Global 500 companies across industries, including financial services, healthcare, government, telecommunications, and more. F5 extends its leadership and innovation today with a converged approach that unifies high-performance app delivery and comprehensive app and API security with one platform that provides holistic visibility, automation, and AI-driven insights.

F5 solutions work across data centers, public clouds, and edge environments, meeting teams where their applications run. With a broad ecosystem of partners and deep experience in highly regulated industries, F5 is trusted by enterprises, telecommunications service providers, and public agencies. Together with you, F5 is building a better digital world—one where every application runs as intended: fast, available, and secure. F5 ADSP is the premier platform engineered for the AI era and built to simplify operations while delivering the strongest app and API security.

F5 ADSP functionality

F5 ADSP converges four disciplines—global application delivery, comprehensive application and API security, unified observability, and automation with programmability—into one platform that helps unify app delivery and security while connecting apps across any environment.

F5 ADSP improves app security and reliability while helping your organization more easily adopt innovations such as cryptography and extensive AI-enablement. Instead of manually stitching together single-purpose tools designed for different environments, F5 ADSP empowers teams to standardize once and scale everywhere.

How F5 ADSP can work for you

- Its **centralized SaaS console** will provide a single operational view of application health, performance, configuration, and security postures across hybrid multicloud environments.
- It will provide a **unified control plane** that keeps enforcement and insights consistent across distributed environments.
- Its **programmable data plane and API-first workflow** will enable automation, integration with CI/CD practices and platform engineering, and rapid adaptation to new requirements.
- **Lightweight agents and connectors** will extend visibility and control near services where proxies can't run—improving coverage across complex, distributed environments.

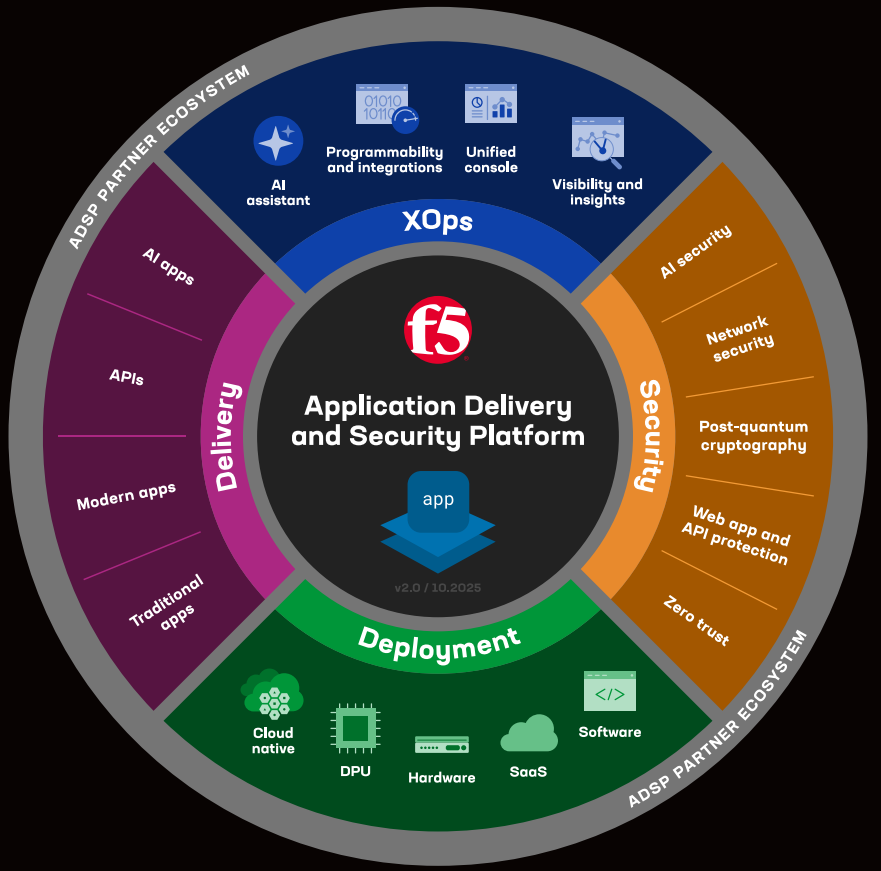


Figure 5: F5 ADSP unifies delivery and security services into a programmable platform that accelerates deployment into any environment and centralizes telemetry for more efficient and more agile operations and innovation.

F5 ADSP business benefits

Improved app performance, reliability, and scalability

App performance and availability form the foundation for sustained customer trust. F5 ADSP brings global traffic load balancing, resilient DNS, multicloud networking that connects applications (not just networks), and acceleration patterns (including CDN) into one framework. That makes it easier to provide service-level connectivity and policy enforcement with shared service discovery, consistent security groups and labels, and a common identity for services moving between clouds and other deployment environments.

Deploy F5 ADSP in any form factor—including hardware, software, virtual appliances, and SaaS; DPU-accelerated paths for data-heavy or AI workloads; and cloud-native ingress/egress—to ensure policy alignment with holistic visibility across every app and API in any environment.

Converged delivery and security

F5 ADSP provides telemetry and data-driven insights so you can continuously enhance application performance, resilience, and security for consistent user experiences. Delivery decisions are guided by signals such as latency, saturation, and health, while being enhanced by anomaly detection for proactive rerouting and autoscaling. Platform-aware agentic threat intelligence and baseline protections included with the delivery infrastructure keep your critical infrastructure protected from malicious threats. F5 is adding automation and agentic intelligence to meet these demands.

The platform also provides full API lifecycle security alongside a comprehensive WAAP stack: WAF services for application-layer attacks, defenses against automated attacks to stop fraud and abuse, and DDoS protection at both the network and application layers. Identity-aware policy enforcement travels with real-time risk assessments. For AI applications, F5 ADSP will support guardrails around prompts and responses, data redaction or sanitization, AI red teaming, and model-aware routing patterns to maintain high throughput and control sensitive information.

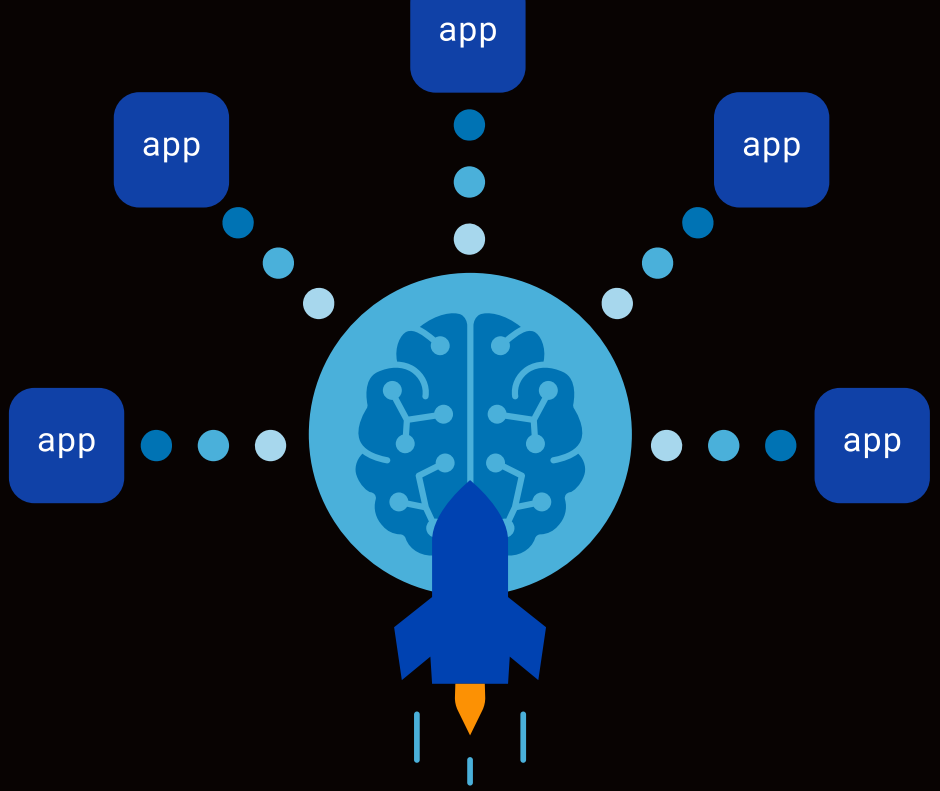
Furthermore, F5 ADSP helps you evolve your cryptography with support for today's most advanced ciphers and efficient key exchange while providing a clear pathway to adopt pending post-quantum cryptographic standards. As typical certificate lifetimes shorten, the platform fully automates their lifecycles (including issuance, rotation, and revocation). This enables rapid, agile app delivery and prevents costly outages caused by expired certificates.

Unified observability and insights

Visibility is most useful when it is shared and actionable. F5 ADSP's SaaS console will correlate telemetry from delivery and security components (health, performance, configuration changes, and security events) into a portfolio-wide view so teams can go from symptom to root cause without changing tools. Dashboards will highlight critical metrics (such as availability, latency, API posture, and policy drifts) and provide guided recommendations. An AI assistant will help operators generate reports, identify and mitigate vulnerabilities, develop and customize scripts, and draft policy updates more quickly, turning intent into action with less friction.

Simplified IT operations

Consistency is the antidote to complexity. F5 ADSP will provide a common user experience and shared workflows across F5® BIG-IP®, F5® NGINX®, and F5® Distributed Cloud Services solutions, so operators don't need to relearn infrastructure configuration procedures. Policy-as-code and API-first interfaces support GitOps practices and CI/CD integration. Lifecycle automation reduces manual steps that cause policy drift. Templates and reusable policies accelerate safe change, while centralized evidence (who changed what, when, and why) makes audits routine instead of disruptive.



App delivery for the AI era

AI model training and inference change the math of app delivery. Large objects move in parallel to storage, and inference endpoints must balance GPU utilization while honoring service level objectives (SLOs) for latency. In that context, F5 ADSP provides an AI app delivery framework that will enable you to:

- Optimize object throughput for training pipelines without starving other services
- Steer inference calls based on model availability, cost, and accuracy SLAs
- Establish guardrails (such as quotas or isolation) so bursty AI jobs don't trample business-critical apps

How F5 ADSP delivers value by industry

Financial services and fintech

Gain consistent security policies plus comprehensive malicious bot defense across digital channels—protecting logins, payments, and sensitive data while maintaining low-latency account holder experiences and providing more streamlined audit processes.

Healthcare

Secure EMR systems, improve patient portal performance and reliability, readily scale, strengthen PHI protection, and ease audits with centralized policy deployments and compliance evidence.

Manufacturing

Secure edge or plant applications and supplier APIs to ensure reliable site-to-cloud delivery with standardized controls.

Retail and e-commerce

Protect critical business logic to prevent data breaches, account takeovers, and fraud while securing peak scalability for launches and seasonal surges.

Public sector and education

Simplify operations for lean IT teams while ensuring resilient DNS and DDoS defense to ensure continuous availability of public services. Centralized reporting helps you satisfy regulatory mandates with less effort.

Technology

Streamline the foundational technology stack with highly differentiated infrastructure and security services that accelerate time to market, protect customers, and facilitate AI innovation. Capitalize on a programmable data plane and agent coverage for microservices across multicloud deployments, while optimizing data paths for AI training and inference without starving other services.

Telecommunications

Obtain high-performance delivery and firewalling at scale, with consistent policy enforcement across regions and edge sites.

Five differentiating capabilities of F5 ADSP

F5 ADSP is engineered for the AI era, and F5 continues to invest in innovative capabilities that showcase the value of a platform-centric strategy. Key differentiators include:

1. A SaaS management console that centralizes and unifies telemetry, policy, and automation. Users will gain a single interface to observe, decide, and act across application delivery, security services, and AI workloads—from enterprise gateways to lightweight, developer-friendly ingress and web servers.

- F5 ADSP treats policy and telemetry as shared assets across locations, enabling policies to be authored once and propagated where needed to reduce drift.
- With standardized telemetry, app and API metrics will carry the same meaning across environments, enabling clear SLOs and faster triage.
- Without switching contexts, operators will be able to view application health, performance, and security postures; author and reuse policies; collect audit evidence; and automate routine tasks. This helps teams reduce issue resolution time, shorten change windows, and strengthen governance.

2. Technology integration for consistent deployments across environments. F5 ADSP runs where your apps live—data centers, multiple public clouds, edge sites, and AI factories—so teams don't have to rearchitect to gain consistency.

- SaaS-delivered capabilities will provide global reach with a single management plane, while agent and connector options will cover diverse runtime environments.
- Shared policy and telemetry will enable standardized operations while respecting environment-specific requirements and constraints.

3. Integrated programmability. Secure and consistent APIs will enable platform automation. For performance-critical or custom logic, F5 will provide a secure WebAssembly (Wasm) you can use to safely extend platform capabilities at line rate. Platform teams will be able to embed security into pipelines, operators can codify change through policy, SecOps teams save time with automate responses, and developers will be enabled to build on secure-by-design paved paths.

4. Best-of-breed capabilities. The platform will provide a unified operator experience for market-leading F5 app delivery and security services. Teams will benefit from a common way to operate while retaining deep efficacy for WAAP (including WAF, bot defense, and DDoS protections), API discovery and protection, access security, high-performance firewall services, traffic management, and more. This convergence shortens learning curves, reduces misconfigurations, and improves observability and control.

5. Agent-based app delivery and security. Lightweight agents and connectors will extend traffic management, discovery, telemetry, and enforcement to wherever your code runs—a flexibility that's especially valuable for microservices, legacy estates, and distributed deployment environments. Expand coverage to shadow and fast-changing services, improve analytics, and bring policy closer to workloads without disruptive topology changes.

These five capabilities and their breadth of functionality set F5 ADSP apart from point solutions and current platform approaches to application delivery and security today.

Get started

The best way to evaluate the potential of F5 ADSP is to see it in action. Most organizations begin with a short reference architecture briefing and a focused pilot that exercises both delivery and security functionality. Guided demos and sandboxes are available. Let's work together to establish a better operating model, prove it with a pilot, and help you scale with confidence.

Actions you can take to learn more:

- Explore F5 ADSP online
- Attend our next AppWorld event for the latest news and innovations
- Contact us for a personalized consultation

Platform starting points by industry

Financial services and fintech

Focus on login and payment processes and business logic, protection from automated attacks, and API governance.

Public sector and education

Start with DNS and DDoS resilience for citizen services and set up centralized dashboards and audit exports.

Telecommunications

Validate performance and policy isolation at scale and plan region-by-region rollouts.

Technology, retail and e-commerce, healthcare, and manufacturing

Tailor implementation to start with critical business flows, whether that means product and feature deployment, partner APIs, checkout processes, customer portals, or plant OT.

ABOUT F5

F5, Inc. (NASDAQ: FFIV) is the global leader that delivers and secures every app. Backed by three decades of expertise, F5 has built the industry's premier platform—F5 Application Delivery and Security Platform (ADSP)—to deliver and secure every app, every API, anywhere: on-premises, in the cloud, at the edge, and across hybrid, multicloud environments. F5 is committed to innovating and partnering with the world's largest and most advanced organizations to deliver fast, available, and secure digital experiences. Together, we help each other thrive and bring a better digital world to life.