Mar 11, 2026

F5 Advances Enterprise Application Security for the AI and Post-quantum Era

New security innovations in the F5 Application Delivery and Security Platform unify AI-driven...
New security innovations in the F5 Application Delivery and Security Platform unify AI-driven protection, zero trust access, and post-quantum readiness across hybrid multicloud environments

LAS VEGAS--(BUSINESS WIRE)-- Today at AppWorld, F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, unveiled new security capabilities that strengthen protection for AI-driven and modern applications. Integrated within the F5 Application Delivery and Security Platform (ADSP), the innovations unify intelligent threat protection, zero trust access controls, and crypto-agile architecture to help enterprises secure distributed applications and prepare for emerging post-quantum risks.

“Security teams do not need more alarms. They need fewer gaps,” said Kunal Anand, Chief Product Officer at F5. “ADSP closes the loop from finding risk to enforcing protection. That includes moving from identified AI model vulnerabilities to validated runtime guardrails, AI-powered risk scoring, and a practical path to zero trust and post-quantum readiness. The point is simple: move faster while reducing your threat landscape.”

AI-driven protection for modern threats

As organizations scale applications across data center, hybrid multicloud, and edge environments, they need faster, more intelligent responses to emerging threats. F5 addresses this through AI-powered protections in the F5 ADSP, automating risk-based web application firewall (WAF) capabilities that reduce operational overhead and improve threat detection, bridging the gaps between risk identification and mitigation.

New to the F5 ADSP, F5 AI Remediate closes a gap between identifying AI model vulnerabilities with F5 AI Red Team and enforcing validated runtime protections with F5 AI Guardrails. AI Remediate accelerates time to response by automating the creation, optimization, and validation of targeted guardrail packages, enabling security teams to put evidence-backed protections into production with human approval. As part of the ADSP, AI Remediate helps organizations reduce exposure quickly without disrupting live AI applications, eliminating repetitive tasks while supporting accountable AI adoption.

Additionally, the latest F5 Distributed Cloud WAF release introduces AI-powered risk scoring, transforming manual processes into automated protections. With outcome-based blocking policies, CISOs, SecOps, and NetOps teams can eliminate threats, reduce operational burden, and achieve rapid time to protection, all while maintaining low false positive rates through layered analysis. F5 Web Application and API Protection (WAAP) solutions such as this minimize reliance on signature-level exceptions and tedious tuning for enterprises with significant application portfolios. Whether safeguarding on-premises hardware or virtual systems, cloud-based SaaS applications, or containerized deployments, F5 enables consistent, enterprise-grade security across ecosystems.

Security in the age of agentic AI

F5 is introducing powerful capabilities within F5 Distributed Cloud Bot Defense to address the emerging challenges of AI-driven automation. These enhanced features combat analytics distortion, automated abuse, and impersonation attempts created by AI agents—threats that increasingly impact both users and the business.

Within the F5 ADSP, Distributed Cloud Bot Defense now offers deeper visibility across application traffic, clearly distinguishing humans, bots, and AI agents. Only trusted, verifiable AI agents are allowed to interact with applications, ensuring malicious or ungoverned activity is blocked while enabling safe, controlled agentic commerce. With unified governance and consistent policy controls for human, bot, and AI agent interactions, these new capabilities help organizations safeguard revenue from harmful automation and confidently participate in the emerging agentic economy.

ADSP also now integrates F5 Distributed Cloud Web App Scanning with F5 BIG-IP Advanced WAF, delivering scalable, automated vulnerability detection for BIG-IP customers. Security teams can identify threats through automated penetration testing and rapidly deploy precise virtual patches. This integration streamlines vulnerability detection and exploit response, reducing time to protection. This approach showcases F5's platform advantage: unified security across hardware, software, and SaaS, offering unmatched flexibility to protect applications and APIs in any environment.

Unified zero trust across hybrid multicloud environments

F5 is evolving BIG-IP Access Policy Manager (APM) into BIG-IP Zero Trust Access, emphasizing its zero trust application access (ZTAA) capabilities as part of the ADSP. Unlike SaaS-based zero trust network access (ZTNA) solutions, BIG-IP Zero Trust Access delivers hybrid zero trust operations with continual identity- and context-aware policy enforcement for modern, cloud, SaaS, and legacy applications. With per-request validation limiting horizontal movement, it strengthens application security across diverse access environments—supporting Identity Aware Proxy, SSL VPN, or IPsec VPN on a post-quantum cryptography (PQC)-ready platform. BIG-IP Zero Trust Access provides a seamless path to adopt zero trust principles while extending F5's ADSP vision.

New API discovery and security options within F5 Distributed Cloud API Security provide flexibility and control for modern, hybrid application environments. Enhancements include out-of-band discovery across multiple data planes, including BIG-IP, NGINX, Kong, and Apigee. Additionally, F5 is also introducing a deployable API security software solution for air-gapped, highly regulated, and cloud-constrained environments. This empowers organizations to maintain full API visibility and oversight without external connections, meeting compliance and data sovereignty requirements. By integrating seamlessly with existing architectures, F5 extends its ADSP vision with API discovery and security that fits any environment without disrupting application performance or workflows.

Building for what’s next: Crypto-agility and post-quantum readiness

F5 is reinforcing its leadership in PQC readiness by delivering a comprehensive, crypto-agile solution within its unified ADSP. By supporting hybrid TLS cipher groups, F5 provides immediate post-quantum security while maintaining compatibility with existing cryptographic workflows—ensuring a practical, standards-aligned approach to future-proofing against quantum threats. As organizations continue to prepare for the eventual arrival of Q-Day by attempting to address quantum-safe requirements, F5 proactively enables seamless quantum resistance today, minimizing long-term risks and supporting security across hybrid

infrastructures.

Collectively, F5's latest security advances deliver on the ADSP promise of seamless application delivery and robust cybersecurity across any deployment scenario. Enterprises benefit from taking a unified platform approach to meeting their security needs.

According to Gartner®, "Organizations should start by evaluating platform solutions first, and many will find that they need to combine a CDN, WAF or API threat protection solution with an API gateway. Again, the key is to look for existing platforms that can be extended or new platforms that offer significant combined capabilities across protection categories. This approach minimizes the number of moving parts and prevents 'proxy overload,' which can lead to excessive performance and availability risk."[1]

With F5's platform-based approach, enterprises gain extended choice to meet their users where they operate, securing applications across hybrid cloud, multicloud, edge, or on-premises ecosystems—all while reducing complexity and time to action. Further details are available in an additional press release focused on the F5 ADSP.

Supporting materials

Blog: F5 AI Remediate: Closing the AI security gap
Blog: API security without compromise: Introducing flexible new discovery options with F5 API security
Blog: Hello, F5 BIG-IP Zero Trust Access
Blog: F5 extends NIST-compliant PQC cipher support

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.

For more information visit f5.com
Explore F5 Labs threat research at f5.com/labs
Follow to learn more about F5, our partners, and technologies:
Blog | LinkedIn | X | YouTube | Instagram | Facebook

[1] Gartner, Implement Effective Application and API Security Controls, April 10, 2025

###

Source: F5, Inc.

View source version on businesswire.com: https://www.businesswire.com/news/home/20260311660169/en/

Dan Sorensen
F5
(650) 228-4842
d.sorensen@f5.com

Holly Lancaster
We. Communications
(415) 547-7054
hlancaster@wecommunications.com

Source: F5, Inc.