NEWS RELEASE

F5 Accelerates Virtual Patching to Manage Emerging Cyber Risks With AI-Powered WAF and Runtime Security

2026-09-01

Frontier AI turns vulnerabilities into exploits in hours; F5 enables security teams to maintain availability, governance, and operational stability by blocking threats in minutes

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, today announced innovations to block frontier AI-driven threats in the data path and enable faster virtual patching, giving security leaders time to make intelligent risk-based decisions rather than reactive operational compromises. With new features such as anomaly detection and agentic threat intelligence, F5's AI-powered web application firewall (WAF) is uniquely capable in delivering real-time protections because of its strategic position in customers' infrastructure. Enhancements to **F5 WAF for Distributed Cloud** and virtual patching provide the precision needed to confidently block active exploits at the request level.

"Frontier AI has collapsed the time between vulnerability discovery and active exploitation," said Kunal Anand, Chief Product Officer at F5. "The old model of waiting for code to be rewritten, tested, and redeployed cannot keep pace. F5 puts protection directly into the data path, where we can identify and block exploits in minutes. Virtual patching gives organizations something increasingly scarce in cybersecurity: time. Time to understand the risk, protect the business, and fix the underlying vulnerability without forcing teams into a permanent state of crisis."

F5 blocks exploits with runtime security, enabling customers to quickly deploy virtual patches. **Introduced** earlier

this year, F5's AI-powered WAF has already seen strong customer adoption. In internal F5 testing, the solution delivered 98% threat detection efficacy while reducing false positives to 1%, extending the **F5 Application Delivery and Security Platform** (ADSP) and giving teams confidence to convert scanner findings into enforced protection in minutes rather than weeks.

F5 has enhanced its capabilities, adding anomaly detection and agentic threat intelligence to a WAF solution that evaluates requests inline using real-time machine learning classification and a neural network risk engine to assign a risk score to each request as it arrives. Scoring risk dynamically, rather than matching known signatures, allows the WAF to help defend against zero-day attempts, injection attacks, and polymorphic exploit chains that change shape on every attempt.

In tailoring infrastructures for a post-Mythos world, F5 helps customers evolve their AI cybersecurity capabilities:

Continually analyze traffic for attack signals

Built directly into F5 WAF for Distributed Cloud, innovative anomaly detection is an intelligent, self-learning capability that continuously analyzes each application's unique traffic patterns, establishing traffic norms and flagging meaningful deviations that could signal a pending attack. It builds per-application statistical baselines and, in real time, scores incoming requests against baselines to identify attacks and false positives. Anomaly detection provides security teams with more accurate protection for their apps without adding complexity.

Prioritize potential exploits with agentic threat intelligence

Security teams do not lack alerts. They lack context. New agentic threat intelligence capabilities, built on technology from the acquisition of Fletch, combine external intelligence on emerging and actively exploited threats with what F5 sees reaching customer applications. Teams get one view of which threats are real, which are relevant to their environment, and what to do about each one, with recommended mitigations that can be applied immediately as virtual patches.

Enforce virtual patches in minutes

Protection cannot wait for a code release. F5 also delivers automated virtual patching with **F5 Distributed Cloud Web App Scanning** (WAS). The solution identifies exposed vulnerabilities, unprotected APIs, and business logic flaws to trigger targeted virtual patches at runtime. For hybrid environments, these timely virtual patching capabilities also extend to F5 WAF for BIG-IP. Customers can apply existing signatures or write custom rules scoped to a specific CVE, attack path, method, header, or parameter across environments.

Balance business risk with emerging threats

False positives are the reason most WAFs sit in passive monitoring mode. F5 WAF for Distributed Cloud, through AI-powered risk-based scoring, reduces false positives to 1%, giving SecOps the confidence to start blocking risky traffic sooner without affecting application availability. Virtual patching using F5 WAF for Distributed Cloud then acts as a safety valve, holding protection in place while developers build, test, and release a permanent fix inside standard change controls.

Extend remediation to the F5 estate

While virtual patching holds the line in the request path, **F5 Insight for ADSP** accelerates patching of the underlying infrastructure. F5 Insight gives operations teams supported update and patching workflows across F5 hardware and software environments with readiness checks, taking advantage of F5's updated **hardened release cadence**. Together, these capabilities mitigate exposure in minutes and remediate the fleet on a preferred schedule.

New AI-powered WAF capabilities are available now on Distributed Cloud as part of the F5 ADSP. Virtual patching capabilities, along with the integration between F5 Distributed Cloud WAS and F5 WAF for BIG-IP, are also available today. Agentic threat intelligence and anomaly detection are rolling out to F5 WAF for Distributed Cloud customers, with broader availability continuing over the coming months.

Supporting resources

- Blog:**F5's AI-powered WAF advances virtual patching for the post-Mythos era**
- Blog:**Four reasons not to miss the F5 post-Mythos security summit**
- F5 virtual security summit:**Security for the post-Mythos world**
- Use case:**Virtual patching is your first line of defense**

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**

Source: F5, Inc.

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

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

Source: F5, Inc.