NEWS RELEASE

F5 Expands AI-powered WAAP Solutions to Arm Enterprises Against Frontier AI Threats and Stop Attacks Before Exploitation

2026-06-09

AI-powered WAF, air-gapped API discovery and security, and virtual patching solutions give enterprises preemptive protection as frontier AI changes the exploitation of vulnerabilities

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, today announced new **web application and API protection** (WAAP) capabilities for its **Application Delivery and Security Platform** designed to keep enterprises ahead of a rapidly shifting threat landscape. Frontier AI models have collapsed the window between vulnerability discovery and active exploitation, giving threat actors faster, cheaper, and more available means of attack. F5 has expanded its industry-leading WAAP solutions, expanding its AI-powered WAF functionality in **F5 Distributed Cloud Services** to directly address that reality.

“Frontier AI has collapsed the window between discovery and exploitation. Attackers no longer need a CVE. They need a model and a target. We built a risk engine that learns continuously and scores every request dynamically, catching attack patterns before a signature exists to stop them. As APIs become the connective tissue for AI inference, we’ve extended that same security posture to air-gapped and on-prem environments, because the most sensitive workloads can’t phone home to the cloud,” said Kunal Anand, Chief Product Officer at F5.

Enhanced AI-powered WAF: Stop attacks before they can be exploited

Enterprise AI security challenges are systemic. According to **F5's 2026 State of Application Strategy Report**, 88% of organizations report at least one AI-related operational or security challenge. To overcome such issues, enhanced AI-powered capabilities in **F5 Distributed Cloud WAF** move beyond signature matching by combining attack indicators with a neural network that is continuously trained on broad, real-world telemetry. Every request receives a numerical risk score built from multiple signals, surfacing novel exploit patterns with the ability to kill CVE chaining at Layer 7, before signatures exist to catch them. In addition to finding new attacks, the solution helps SecOps teams reduce operational complexity, resulting in fewer false positives, less manual tuning, and faster response.

F5's approach is validated by recent **SecureIQLab testing**, where F5 WAAP and **F5 AI Guardrails** achieved a 97.09% total security score, including 100% accuracy against key risks listed in the OWASP WAF Top 10 and API Top 10, as well as perfect scores for bot attack mitigation and Layer 7 DoS protection. F5's AI-powered WAF is used by the world's largest enterprises, highlighting the urgency of securing today's applications.

Key capabilities of F5's AI-powered Distributed Cloud WAF include:

- Numerical risk scoring: Dynamic, multi-signal scores on every request give security teams precise, actionable context rather than a binary block-or-allow decision
- Continuously trained shared model: The risk engine learns from multiple factors, including high-confidence signatures and attack indicators, so detections improve as the threat landscape evolves
- Pre-exploit detection: Behavioral signals trained to reason like attackers are designed to identify attack activity before threats are formally classified, addressing a window that signatures and patches cannot reach

Introducing F5 API Security Local Edition: API discovery and protection for air-gapped and regulated environments

Organizations in highly regulated and sensitive industries, such as defense, intelligence, government, financial services, healthcare, and critical infrastructure, operate in environments where cloud-based security tools may not be an option. With the rapid adoption of AI, APIs have become even more critical, but they also bring increased security risks. APIs are the gateways for AI inference and data processing, making them a growing target for malicious activity. Until now, those environments have had limited access to the on-premises API discovery and security they need.

F5 API Security Local Edition addresses this by delivering comprehensive API visibility, governance, and security entirely on premises, without relying on external services or cloud connectivity. This ensures organizations can safeguard their APIs, and the AI systems they power, against today's evolving threats, with no dependency on external services or cloud connectivity.

As **digital sovereignty** requirements accelerate demand for on-premises security options across regulated industries, air-gapped solutions are emerging as a key component of how organizations meet those requirements. Key capabilities of F5 API Security Local Edition include:

- API discovery and visibility automatically identify API endpoints, map schemas, and surface security risks with no cloud dependency.
- Risk scoring and blocking dynamically evaluate API risks and identify potential threats in real time, enabling the discovery, documentation, and monitoring of APIs effectively.
- Seamless integration with **F5 BIG-IP Advanced WAF** provides the enforcement point for rapid blocking of malicious or unknown APIs. It supports seamless policy updates and exporting validated documentation for implementing a positive security model. This integration ensures unmatched API protection on premises.
- Local deployment and on-premises management deliver local analysis and visualizations via a dedicated console operated entirely within an organization's on-premises infrastructure.

Virtual patching: Close the window between discovery and protection

In a world where frontier AI models are constantly probing for vulnerabilities, previous timelines of exploitation and remediation no longer apply. There needs to be a way to identify a potential stopgap to deter exploitation and provide a window of opportunity for organizations to patch vulnerabilities that face imminent exploitation.

The combination of BIG-IP Advanced WAF and **F5 Distributed Cloud Web App Scanning** can determine and then apply a virtual patch targeting protections at the application delivery layer from the moment a vulnerability is identified. The F5 solution keeps applications protected at runtime while patching and remediation work their way through development and testing cycles and, ultimately, into production. This approach is designed to buy organizations valuable time to address vulnerabilities before they can be exploited.

Protecting every app and API in every environment

AI-accelerated exploitation, pre-CVE attacks, and the challenge of securing isolated environments are not future risks—they reflect current enterprise threats. The capabilities announced today extend the F5 Application Delivery and Security Platform to meet the threats that security teams in critical industries face, while reinforcing F5's commitment to protecting apps and APIs in any environment.

Supporting materials

- Blog:**Securing our code with frontier AI: What F5 built and learned**
- Blog: **Why risk scoring matters in the age of AI-driven vulnerability hunting**

- Blog:**Virtual patching in practice with F5 BIG-IP Advanced WAF and F5 Distributed Cloud Web App Scanning**
- Blog:**API security risks persist across all environments, even when air-gapped**
- Resource:**Frontline defense for frontier AI threats**

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.