NEWS RELEASE

F5 Distributed Cloud Bot Defense Adds Device Intelligence and Agentic AI detection to Guard Against Automated Account Abuse

2026-09-15

New multi-signal risk decisioning, persistent device identification, and agentic AI protections in F5 Distributed Cloud Bot Defense give enterprises greater visibility and control

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, today announced enhancements to **F5 Distributed Cloud Bot Defense**, introducing new device intelligence capabilities and specialized agentic AI protections. Together, these capabilities bring persistent device context and continuous risk decisioning to application security, giving organizations the real-time agent management designed to help welcome trusted digital interaction while helping stop automated fraud and abuse.

These updates arrive as AI agents emerge as a key channel for interacting with websites, mobile applications, and customer portals. Unlike basic web crawlers or simple automated scripts, AI agents perform autonomous, multi-step actions on behalf of consumers—such as executing transactions in agent-based commerce, booking travel, and conducting banking operations. Because these agents interact directly with APIs at machine speed, first-generation bot management tools built around rigid “bot or not” rules are quickly overwhelmed. Static, request-level controls can no longer distinguish between authorized AI driving legitimate business and malicious bots attempting fraud, while blunt IP blocking or CAPTCHAs risk shutting down revenue-generating AI channels.

F5 addresses this challenge by delivering advanced bot defense as a core component of its **web application and**

API protection (WAAP) offerings, integrated with the **F5 Application Delivery and Security Platform** (ADSP). Rather than relying on single-request inspection, F5 correlates behavioral, device, and client-integrity telemetry across interactions. This multi-signal approach establishes trust at critical login, web, and API connections without disrupting legitimate users or authorized AI agents.

“Agentic AI is breaking the old security model, where automated traffic was treated as inherently malicious,” said Kunal Anand, Chief Product Officer at F5. “The answer is not to block AI. It is to understand which agents and devices can be trusted, what they are trying to do, and how risk changes across every interaction. By bringing persistent device intelligence and real-time risk decisioning into the active data path, F5 helps organizations stop fraud and account abuse without closing the door on legitimate users, trusted AI agents, or new digital business models.”

Key enhancements to F5 Distributed Cloud Bot Defense include:

- Persistent device identification: Identifies and tracks devices across multiple sessions and accounts, exposing hidden abuse patterns such as multi-account access, credential stuffing, and account takeover.
- Real-time device risk scoring: Evaluates client integrity signals in real time to detect suspicious environments (including emulators, device spoofing, and tampering).
- Risk-based workflow enforcement: Enables customers to set dynamic policy actions (allow, step-up challenge, rate-limit, or block) intended to help reduce disruptive CAPTCHA friction and false positives for real users and approved automation.
- Agent-aware policy framework: Classifies and manages traffic from humans, trusted AI agents, and malicious bots within a single policy framework on the F5 ADSP, helping organizations adopt AI-driven workflows with confidence.

Availability

New agentic AI protections for F5 Distributed Cloud Bot Defense are available today. The device intelligence functionality is currently expected to reach limited availability for F5 Distributed Cloud customers in the fourth quarter of calendar year 2026, with broader availability expected thereafter over the coming months.

Supporting resources

- Blog:**Who can you trust in the age of AI agents?**
- Product page:**F5 Distributed Cloud Bot Defense**
- F5 virtual security summit:**Security for the post-Mythos world**
- Analyst report:**Protect agentic commerce to prevent abuse and preserve revenue**

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**

Forward-looking statements

This press release contains forward-looking statements, including regarding the expected availability, timing, functionality, and benefits of F5 Distributed Cloud Bot Defense and device intelligence features, made under the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Actual results could differ materially due to the risks described in F5's SEC filings, including its most recent Forms 10-K and 10-Q. F5 undertakes no obligation to update these statements.

F5 and F5 ADSP are trademarks, service marks, or tradenames of F5, Inc. or its affiliates in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners.

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.