



NEWS RELEASE

F5 Named a Leader in the 2026 IDC MarketScape for Worldwide WAAP Platforms for the Second Time

2026-10-01

IDC MarketScape notes F5's key strengths including AI-powered WAF with a measurable efficacy gain, breadth of AI security options, and AI assistance and programmability

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, today announced it has been named a Leader in the IDC MarketScape: Worldwide WAAP Platforms 2026 Vendor Assessment (US54130626, September 2026)¹. This marks the second time F5 has been recognized as a Leader, including the prior assessment in 2024.

Organizations today face frontier AI threats and autonomous agentic attacks. Autonomous AI models can scan, discover, and exploit vulnerabilities at machine speed. With the vulnerability exploit window now inverting to negative 7 days, attacks routinely begin before a software vendor even releases a patch. The proliferation of shadow AI and zombie APIs introduces exposure to new risks and the possibility of data leakage. And CISOs must now deal with the long-term exposure of "harvest now, decrypt later" quantum attacks. Security leaders need to defend every app, API, and AI model, everywhere, with consistent policy, less complexity, and AI-powered defenses. With capabilities like **virtual patching**, F5's web application and API protection (WAAP) solution is built to help them reduce risk, strengthen resilience, and enforce policy—wherever their apps and APIs run.

"We've entered an era where reactive defenses and traditional patch cycles simply can't keep up," said John Maddison, Chief Marketing Officer, F5. "Organizations trust F5 to protect what matters most and help them

innovate with confidence. Being named a Leader once again in the 2026 IDC MarketScape for WAAP reflects our continued leadership and investment in AI-powered security. With capabilities to close the loop from proactive vulnerability discovery to automated virtual patching in minutes, we stop machine-speed attacks during runtime, buying development teams critical runway. The threat landscape will keep evolving, and so will we, as we help our customers defend every app, API, and AI model, wherever they run.”

Why we believe F5 was named as a Leader

F5 is among the only security providers delivering an application delivery and security platform purpose-built to secure modern applications, APIs, and AI—from development through runtime, across any environment. F5’s enterprise WAAP solution, delivered as part of the **F5 Application Delivery and Security Platform (ADSP)**, converges web application firewall (WAF), API security, bot defense, and DDoS mitigation capabilities to reduce gaps and tool sprawl wherever apps and APIs live.

In its assessment, IDC MarketScape noted several of F5’s key strengths, including:

- AI-powered WAF with a measurable efficacy gain. F5 WAAP balances a combination of signatures and analysis to increase detection accuracy and reduce false positives without the need for constant manual tuning. F5 customers reported that the addition of the neural-network risk engine cut false positives and lifted detection accuracy measurably. The new engine further aids F5’s efforts to detect zero days in a more timely manner, including the Ivanti EPM and SolarWinds Web Help Desk CVEs.
- Breadth of AI security options. The F5 suite for AI includes **F5 AI Red Team**, **F5 AI Guardrails**, and **F5 AI Remediate**. F5 AI Red Team provides proactive testing of AI applications for vulnerabilities. F5 AI Guardrails provides the real-time inspection and monitoring needed to block threats targeting AI, such as prompt injection and data leakage. Importantly, remediation adds a crucial element to other AI security solutions, e.g., AI Red Team and AI Guardrails, as it allows organizations to close the loop on security events.
- Bot and agent defense built on rich telemetry. F5 bot defense collects 120+ signals through tamper-resistant client-side instrumentation, and now distinguishes humans, bots, and AI agents, gating action to verified agents via Web Bot Auth and a Skyfire KYA (Know Your Agent) partnership.
- Air-gapped API security supports government and other sensitive customers. **F5 API Security Local Edition** deploys without external connectivity and enforces directly on BIG-IP, which is important for security and privacy-aware agencies and organizations.

“As AI reshapes both the threat landscape and the tools available to defend against it, enterprises need WAAP platforms that reduce complexity while keeping pace with machine-speed attacks. F5’s ability to converge AI-powered WAF, API security, bot defense, and AI-specific protections into a single unified platform is a key reason it stands out in this year’s assessment,” said Chris Rodriguez, Research Director, Security & Trust, IDC.

F5's AI security provides highly effective protection for organizations with 99.3% prompt-injection block efficacy validated by **SecureIQLab**. And protection has recently been extended across the entire AI lifecycle with our introduction of **F5 Workforce AI Security** to discover shadow AI, govern employee use of public and private models, and control autonomous AI agents acting with borrowed authority.

Real-world results across industries

Across banking, insurance, retail, and other regulated industries, organizations rely on F5 WAAP to enforce consistent policy, streamline security operations, and protect apps, APIs, and AI across hybrid, multicloud environments. Today, 28% of F5's top 1,000 customers have already adopted all three deployment modes with F5 defined as SaaS, software, and hardware/cloud—validating that platform consolidation reduces operational sprawl.

A number of customers in highly regulated industries such as financial services institutions use F5's AI-powered WAF to cut through alert noise, reducing the manual tuning that traditionally slows security teams down and giving analysts confidence to move from monitoring to active blocking sooner—critical in an environment where automated, AI-generated attacks move faster than human-led response. Insurers and other API-intensive businesses turn to F5 to gain visibility into sprawling API estates—some managing hundreds of APIs across hybrid environments—helping close blind spots, speed threat detection, and respond to emerging risks with more confidence.

Across industries, customers consistently point to the same operational advantage: simplicity at scale. F5's converged approach to WAAP protects both the application runtime path and the underlying infrastructure fleet via automated update workflows in **F5 Insight for ADSP** across any cloud or data plane, meaning new protections can be deployed in days rather than months, and additional capacity can be added in minutes, not weeks—letting security teams keep pace with growth without adding complexity or headcount.

Supporting materials

- IDC MarketScape excerpt: **F5 was named a Leader in the IDC MarketScape: Worldwide WAAP Platforms 2026 Vendor Assessment**
- Blog: **IDC MarketScape recognized F5 as a Leader in Web Application and API Protection Platforms 2026 Vendor Assessment**
- SecureIQLab validation testing: **F5 AI Guardrails: Validated protection against real-world AI attacks**

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.

About IDC MarketScape

IDC MarketScape vendor assessment model is designed to provide an overview of the competitive fitness of technology and service suppliers in a given market. The research utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each supplier's position within a given market. IDC MarketScape provides a clear framework in which the product and service offerings, capabilities and strategies, and current and future market success factors of technology suppliers can be meaningfully compared. The framework also provides technology buyers with a 360-degree assessment of the strengths and weaknesses of current and prospective suppliers.

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**

F5, F5 ADSP, and BIG-IP 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. The use of the term "partnership" in this press release does not imply a legal partnership, joint venture, or agency relationship between F5 and Skyfire.

Source: F5, Inc.

An excerpt of the IDC MarketScape: Worldwide WAAP Platforms 2026 Vendor Assessment is available for download: **<https://www.f5.com/go/report/f5-named-leader-in-idc-marketscape-enterprise-waap-platforms-2026>**

¹ IDC MarketScape: Worldwide WAAP Platforms 2026 Vendor Assessment (Doc #US54130626, September 2026).

Dan Sorensen

F5

(650) 228-4842

d.sorensen@f5.com

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

Source: F5, Inc.