



Feb 26, 2026

F5 Labs Sets New Standard for AI Security Benchmarking With Model Risk Leaderboards and Threat Intelligence

Comprehensive AI Security Index and Agentic Resistance Score metrics help organizations stress-test...
Comprehensive AI Security Index and Agentic Resistance Score metrics help organizations stress-test security performance of AI systems, from pilot to production

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, today introduced enhanced threat intelligence resources enabling enterprise security leaders to reliably measure and compare the risk profiles of all popular AI models. From the F5 Labs threat research team, Comprehensive AI Security Index (CASI) and Agentic Resistance Score (ARS) leaderboards provide standardized, monthly-updated benchmarks backed by leading research, pairing real-time attack intelligence with expert analysis of evolving AI attack vectors.

Stemming from F5's acquisition of CalypsoAI, these industry-leading security resources include one of the largest AI vulnerability libraries, uniquely updated with more than 10,000 new attack prompts each month, and utilizing over one year of accumulated attack data. F5 Labs now offers enterprises and the wider security community a powerful and consistent means to evaluate, compare, and select AI models and providers prior to production, based on their ability to address key challenges and real-world application security threats.

"Deploying unverified AI models into critical infrastructure is not innovation; it is negligence. Organizations need a way to continuously quantify resilience. F5 Labs AI Leaderboards offer that standard. These rankings isolate specific weaknesses in the model layer, giving security teams the intelligence they need to govern inference and block attacks before they happen," said Kunal Anand, Chief Product Officer at F5.

With enhanced visibility, leaderboards from F5 Labs help security teams holistically identify and shore up vulnerabilities to improve defenses alongside the F5 Application Delivery and Security Platform, from safeguarding APIs and data to preventing DDoS attacks to accelerating DevSecOps through automation and scalability.

Assessing today's AI model landscape

The rapid integration of AI into every facet of business operations has brought with it a requirement for the robust security validation of an organization's chosen models. Designed to help security practitioners answer, "How secure is my model?", F5 Labs' leaderboards establish metrics around the paths of least resistance and minimum compute resources required to complete both simple and complex attacks.

Along with a straightforward ranking, F5 Labs' Comprehensive AI Security Index (CASI) offers metrics such

as:

Average Performance: Baseline model performance measured across standardized tasks under normal operating conditions

Risk-to-Performance Ratio: Insight into the tradeoff between model safety and performance

Cost of Security: The current inference cost relative to the model's CASI, assessing the financial impact of security

Supplementing CASI, F5 Labs' Agentic Resistance Score (ARS) evaluates how AI systems withstand sustained, adaptive attacks by an AI agent tasked with achieving a goal. Rather than attempting to execute one individual prompt, AI agents conduct prolonged interactions with models, applying reasoning and psychological methods in an attempt to bypass security guardrails. ARS assesses AI systems across three core dimensions:

Required Sophistication: The minimum level of attacker ingenuity needed to successfully compromise the AI system

Defensive Endurance: How long the system remains secure under prolonged, adaptive, multi-step attacks

Counter-Intelligence: Whether failed attacks inadvertently expose signals or system behavior that could enable future exploits

Moving beyond a baseline for model security

Today's announcement complements the recent general availability of F5 AI Guardrails and F5 AI Red Team. F5 AI Guardrails allows enterprises to apply both out-of-the-box and custom guardrails to secure how AI interacts with users and data. F5 AI Red Team delivers rigorous testing with waves of autonomous AI agents, simulating a dedicated team of modern security analysts and multi-step attacks that probe, learn, and adapt.

This approach directly informs CASI and ARS leaderboards, enabling F5 to measure both baseline model security characteristics and long-term resistance under continuous, real-world threat conditions. In addition to the CASI and ARS rankings, which are updated every month with the latest scores, F5 Labs also publishes monthly AI Security Insights as companion research. These focused articles explain notable score movements reflected on the F5 Labs AI Leaderboards, cover recent AI news and research, and provide deep-dives on specific AI attacks.

"F5's existing traffic inspection and logging capabilities are expanded with the acquisition of CalypsoAI, adding runtime AI governance capabilities and visibility into AI system behavior. Paired with their security research arm, F5 Labs, that updates CASI and ARS rankings every month, F5 customers are provided with both a useful set of security metrics to consider when selecting an AI model, as well as the tools needed to constrain how AI systems are used, what data they may access, and how outputs are generated," said Grace Trinidad, Research Director, AI Security & Trust, IDC.

F5 Labs AI Leaderboards are just one example of how F5 is helping customers and the security community embrace AI with a broader understanding of evolving attack methodologies and model defenses. By surfacing and aggregating impactful results, F5 is better equipping the global community to address escalating challenges posed by modern cybersecurity threats. In formalizing a ranking system for leading AI models, F5 Labs also encourages further knowledge sharing among security professionals, creating a ripple effect for greater adoption of application security best practices.

Supporting materials

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](#)

F5 is a trademark, service mark, or tradename of F5, Inc., in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners.

Forward-looking statements

This press release contains forward-looking statements, including statements regarding the expected capabilities, benefits, availability, and impact of the F5 Labs AI security benchmarking resources, including the Comprehensive AI Security Index (CASI), Agentic Resistance Score (ARS), model risk leaderboards, and related threat intelligence offerings. These statements are based on current expectations and assumptions and involve risks and uncertainties that could cause actual results to differ materially. Factors that may affect outcomes include customer adoption, product development timelines, competitive conditions, integration of acquired technologies, security vulnerabilities, and broader economic and market conditions, as well as other risks described in F5's filings with the U.S. Securities and Exchange Commission. All forward-looking statements in this press release are based on information available to F5 as of the date hereof and are qualified in their entirety by this cautionary statement. F5 undertakes no obligation to update any forward-looking statements.

Source: F5, Inc.

View source version on [businesswire.com](https://www.businesswire.com):

<https://www.businesswire.com/news/home/20260226568883/en/>

Jenna Becker

F5

(415) 857-2864

j.becker@f5.com

Holly Lancaster

We. Communications

(415) 517-7054

(415) 547-7054
hlancaster@wecommunications.com

Source: F5, Inc.