Mar 18, 2026

F5 Collaborates with AWS and Microsoft on NSS Labs Research Paper on AI Runtime Security Testing

New NSS Labs research sets the standard for evaluating AI security, establishing a blueprint for...
New NSS Labs research sets the standard for evaluating AI security, establishing a blueprint for enterprises

SEATTLE--(BUSINESS WIRE)-- F5, a global leader in delivering and securing every app and API, in collaboration with Amazon Web Services (AWS) and Microsoft, today announced their contributions to a landmark white paper from NSS Labs focused on *AI Security Beyond the Model: What Enterprises Need to Care About—and Why*. This effort lays out a comprehensive framework for running proper AI guardrails efficacy tests, marking a defining moment in AI security and governance best practices.

The white paper aims to provide enterprises with actionable, real-world guidance for understanding and evaluating the security and accountability around AI systems in complex, high-stakes environments.

As AI continues to reshape enterprise operations, it introduces unprecedented risks, expanding attack surfaces that expose organizations to operational, legal, and reputational threats. This white paper addresses the urgent need for standardized methods to evaluate AI security solutions effectively. It represents an industry-first approach to AI security uniting leaders in security, cloud, and AI to address one of the most pressing challenges enterprises face today. The goal of this white paper is to establish industry-wide clarity, structure, and accountability for AI guardrails, ensuring enterprises can adopt AI innovation safely and effectively.

Key recommendations

The white paper delivers an actionable framework for enterprises to understand and implement AI security guardrails. Among its key recommendations, the analysis outlines:

Critical Capability Areas: Identifying the key components enterprises should evaluate, including input threat detection, output data exfiltration management, and agentic AI controls.
Framework for Validation Testing: Providing a blueprint for independent, adversarial, and real-world testing of AI security controls to ensure efficacy under dynamic conditions.
Governance and Operational Resilience: Emphasizing the importance of governance alignment and resilience in handling stress, failures, and degradation within AI systems.

NSS Labs: Rigorous standards for cybersecurity evaluation

“Our research underscores the importance of independent validation for AI guardrails,” said Ian Foo, Chief Technology Officer and EVP of Product for NSS Labs. “AI is transforming global enterprises, and without

rigorous, repeatable validation tests, security claims are just empty promises. We believe this framework will empower enterprises to make informed decisions and set new standards for AI safety."

F5: Advancing AI security through application delivery expertise

"This collaborative effort reflects the critical importance of bringing together diverse expertise from across the industry to address the complex challenges of securing AI systems," said Jeanette Hur, Global Solutions Architect, F5. "At F5, we bring decades of layer 4-7 application delivery and security expertise to this collaboration with NSS Labs, AWS, and Microsoft. This framework will empower organizations to rigorously evaluate AI guardrails, ensuring that enterprises can confidently deploy AI innovations while maintaining resilience, security, and accountability across their application ecosystems."

Microsoft: Ethics and security are not mutually exclusive with AI

"At Microsoft, we're very passionate about advancing AI in an ethical and secure way," said Zachary Riffle, Security Architect, Microsoft. "This white paper is a step forward, and we really hope it provides buyers of all sizes with the right tools and vendor-agnostic guidance to secure whichever AI model or system they use, while maintaining transparency and accountability."

Understanding and securing enterprise AI systems

This white paper provides a practical roadmap for enterprises grappling with the rapidly evolving challenges of AI security. By focusing on what truly matters—real-world efficacy, independent validation, and robust governance—it equips organizations with the knowledge they need to make smarter, more informed decisions when evaluating AI security solutions.

For enterprises leveraging AI, understanding how to protect against emerging risks like data exfiltration, prompt injection, and governance failures is no longer optional. This resource helps security teams move past the noise of vendor claims and gives them the tools to ask the hard questions, evaluate solutions rigorously, and implement guardrails that ensure AI systems remain secure and accountable.

Supporting materials

NSS Labs white paper: AI Security Beyond the Model: What Enterprises Need to Care About—and Why
Blog: Setting the standard: Why AI guardrail efficacy testing can't wait

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.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20260318092868/en/

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

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

Source: F5, Inc.