



NEWS RELEASE

# F5 and Forcepoint Partner to Secure Enterprise AI From Data Creation to Runtime Operations

2026-03-24

Collaboration connects data discovery and classification with runtime protection and continuous assurance to help organizations securely operationalize AI

SEATTLE & AUSTIN, Texas--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, and Forcepoint, a global leader in data security, today announced a new alliance to help enterprises secure AI across its lifecycle—from foundational data discovery and classification through runtime protection and continuous assurance.

As organizations rapidly deploy AI across copilots, assistants, and automated workflows, security practices are struggling to keep pace. Many enterprises face complex challenges in identifying where sensitive data resides, how it flows through AI systems, and the potential risks introduced during production. While data governance, application security, and runtime protections remain crucial, they commonly operate in silos, creating gaps between security policy and AI behavior in practice.

To solve this problem, Forcepoint's AI-native **Data Security Posture Management (DSPM)** data discovery and classification capabilities combine with F5's red teaming and AI guardrails functionality in the **F5 Application Delivery and Security Platform (ADSP)**. This approach provides runtime protections for AI applications, APIs, models, and agents to help organizations operationalize AI safely while maintaining control and visibility over sensitive enterprise data.



The combined capabilities help security teams identify and address data vulnerabilities in real time, prioritize AI use cases based on risk, enforce runtime controls over AI interactions, and monitor systems for misuse or abnormal behavior. Continuous telemetry and policy validation provide ongoing assurance that AI systems are operating securely and in line with enterprise governance requirements.

“Enterprises are moving AI initiatives from experimentation to production faster than most security programs can adapt,” said John Maddison, Chief Marketing Officer, F5. “By combining Forcepoint’s deep data intelligence and contextual awareness with F5’s advanced application security and runtime protections, organizations eliminate operational security gaps with unmatched confidence and control in their AI operations. As AI’s threat surface continues to expand, the combined power of DSPM technologies with F5’s AI Red Team and AI Guardrails equips enterprises with proactive tools to securely scale and govern AI at every stage of its lifecycle.”

“AI has fundamentally redefined data security, exposing static policies for what they are: inadequate,” said Naveen Palavalli, Chief Product and Marketing Officer, Forcepoint. “F5 and Forcepoint are establishing a new standard of continuous, adaptive protection that follows data from the moment of creation through every stage of its lifecycle, including the runtime layer where AI systems operate, evolve, and expand risk vectors. The threats AI brings require a new category for proactive data and AI risk mitigation, and our partnership is delivering on this today.”

## Connecting data intelligence with runtime AI protection

Organizations adopting AI must determine which data should be accessible to AI systems, which use cases present the greatest risk, and how to enforce policies once AI applications are in production. The F5-Forcepoint partnership addresses these challenges by treating AI security as a continuous lifecycle, connecting data understanding with runtime enforcement.

At the foundation, Forcepoint enables organizations to discover, classify, prioritize, and govern sensitive and business-critical data across cloud, SaaS, endpoint, and enterprise data environments. This AI-powered visibility helps determine which data is appropriate for AI use and which initiatives require the highest level of scrutiny.

F5 then secures AI systems at runtime by enforcing policies across APIs, gateways, applications, and AI agents. The **F5 AI Red Team** and **F5 AI Guardrails** functionality within F5 ADSP enables customers to secure AI models through its monitoring and adversarial testing capabilities. By leveraging the solution, customers will defend against threat actors by detecting prompt abuse, preventing data exfiltration, and protecting AI models and workloads from emerging threats.

Together, the companies enable organizations to move from data reality to runtime trust, ensuring AI systems are

grounded in trusted data while continuously protected as they operate in production.

By aligning data security with application and API protection, the F5-Forcepoint partnership provides a pragmatic path for enterprises to adopt AI without rebuilding their security architecture or waiting for fully integrated platforms to mature.

F5 is at the **RSA Conference** this week, where attendees can visit booth #6365 to learn more about the joint F5-Forcepoint solution and related AI security innovations.

Join Forcepoint leaders and experts to explore how organizations are securing data in the age of AI, including the F5-Forcepoint solution, at the Forcepoint Experience Center on the fourth floor of the **St. Regis San Francisco** during RSA week.

## Supporting materials

- F5 blog:[F5 and Forcepoint to secure AI from data to runtime](#)
- Forcepoint blog:[From Data Truth to Runtime Trust](#)

## 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](https://f5.com).

Explore F5 Labs threat research at [f5.com/labs](https://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. The use of the terms “partner,” “partners,” “partnership,” or “partnering” in this press release does not imply that a joint venture exists between F5 and any other company.

## About Forcepoint

Forcepoint enables Self-Aware Data Security, an AI-native approach that helps enterprises and governments know their data everywhere, adapt to evolving risks and regulations in real time, and protect at scale with a unified, single-policy framework. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. For more information visit **Forcepoint.com**; or connect with Forcepoint on **LinkedIn**.

Source: F5, Inc.

Jenna Becker

F5

(415) 857-2864

**j.becker@f5.com**

Holly Lancaster

We. Communications

(415) 547-7054

**hlancaster@wecomcommunications.com**

Rachael Lyon

Forcepoint

**rachael.lyon@forcepoint.com**

Source: F5, Inc.