Mar 03, 2026

F5 Teams With WWT to Help Customers Accelerate AI Adoption Without Compromising Security

F5 now supports AI Readiness Model for Operational Resilience (ARMOR) framework from WWT to better...
F5 now supports AI Readiness Model for Operational Resilience (ARMOR) framework from WWT to better address the expanding AI attack surface

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, today announced enhanced support for WWT's AI Readiness Model for Operational Resilience (ARMOR). Built on practical experience and expert insights, ARMOR is a vendor-agnostic AI security framework delivered by World Wide Technology (WWT), leveraging a jointly built approach with NVIDIA and strengthened through real-world collaboration. Designed to secure AI deployments at every stage, it helps organizations better address the expanded attack surface created by hybrid AI platforms, where data moves constantly between environments, APIs, and new connection points.

The ARMOR framework conceptualizes an advanced, modular cybersecurity solution delivered by WWT to meet the needs of enterprises facing unprecedented growth in the rate, scale, and sophistication of cyberattacks. It focuses on providing AI-powered threat detection, mitigation, and visibility while integrating with industry-leading solutions from the F5 Application Delivery and Security Platform (ADSP). This combination ensures that workloads are deployed and accessed safely and efficiently, no matter where they reside across multicloud environments.

"For organizations of any size, ARMOR provides a scalable framework that can be continuously refined as new partners and technologies join the ecosystem," said Istvan Berko, Global Head of AI Cyber and Innovation at WWT. "By embedding security from chip-to-cloud and aligning with industry organizations and compliance mandates, ARMOR articulates an end-to-end AI security approach that provides comprehensive coverage over key IT domains."

ARMOR is divided into six primary domains to ensure comprehensive, modular coverage of the full AI lifecycle, with "Cyber Resilience" acting as an additional umbrella. Each domain targets a distinct security challenge, enabling organizations to align their defenses with real-world threats, regulatory requirements, and operational maturity for scalable, resilient AI deployments. Within each domain, there are myriad use cases for a variety of F5 offerings, with notable examples included below:

Governance, Risk, and Compliance (GRC) aligns AI operations with regulatory, policy, and ethical standards for transparent and trustworthy AI systems. F5 AI Guardrails acts as a proxy for AI traffic, inspecting prompts and responses to prevent data leakage, mitigate prompt injection, and block other AI-targeted attacks. The solution also provides observability, logging, and traceability features such as watermarking to support compliance and security audits.

Secure AI Operations transforms reactive defenses into proactive strategies, enhancing threat detection,

streamlining incident response, and driving continuous improvement. Aligned with a broader solution focus on XOps, F5 provides real-time fleet observability and recommendations, with F5 web application firewall (WAF) offerings reducing false positives and providing actionable alerts with predictive insights, rapid triage, and automated F5 iRules creation and translation. For enhanced visibility to further drive security and interoperability, F5 products support OpenTelemetry-compatible capabilities across F5's ADSP.

Model Protection details layered defenses like model scanning, runtime security, lifecycle traceability, and red teaming to safeguard AI systems from adversarial threats, misuse, and operational vulnerabilities. F5 AI Red Team automates adversarial testing, paired with F5 AI Guardrails to dynamically protect against prompt injection, jailbreaks, data exfiltration, and model misbehavior while supporting advanced analytics and risk benchmarking.

Secure Development Lifecycle (SDLC) helps define a practical roadmap for secure coding practices, threat modeling, and AI model scanning to better identify, prioritize, and remediate vulnerabilities. F5 ADSP's XOps overlay spans all products, integrating application scanners, automation, orchestration, and AI assistants to deliver consistent advantages across the portfolio while tightly aligning with the SDLC. This creates a virtuous cycle of testing and implementation, as well as a single source of truth—without compromising speed or agility—by treating secure configurations as code to better support SDLC planning, stability, and management.

Infrastructure Security unlocks scalable, risk-based identity security for AI and high-performance computing environments, helping organizations analyze the foundational controls securing their systems. F5's extensive security offerings provide post-quantum cryptography (PQC) readiness. Per-tenant connectivity and enforcement is provided by F5 Distributed Cloud Services, while BIG-IP Next for Kubernetes controls ingress/egress for Kubernetes clusters to apply load balancing, security, visibility, and network integration functions.

Data Protection outlines maturity models, AI-specific strategies, and implementation best practices to help build resilient data security across hybrid environments. F5 ADSP provides security standardization across the control plane, and F5 BIG-IP Local Traffic Manager standardizes secure, structured transport between models and agents while providing high availability and health checks. Additionally, the recent release of F5 BIG-IP v21.0 adds pre-configured S3 profiles, enabling customers to more easily support AI storage use cases while optimizing performance and efficiency.

Cyber Resilience grounds all six of the above domains in zero trust and defense-in-depth principles, with maturity models, recovery planning, and integrated operations to help organizations prepare, respond, and recover. F5 ADSP solution guidance in providing security for every app and API reinforces the companies' shared perspective that every domain has distinct security requirements and must be properly protected.

"AI's ascension and integration into every element of modern business have transformed what application, API, and infrastructure security should look like," said Kunal Anand, Chief Product Officer at F5. "Together with companies like WWT, F5 is focused on helping CISOs and security teams implement game-changing AI capabilities while simultaneously addressing corresponding shifts in overall threat, compliance, and data sovereignty landscapes."

Supporting materials

Press release: World Wide Technology unveils ARMOR: A collaborative AI security framework with NVIDIA AI
Blog: WWT's ARMOR framework accelerates AI adoption with F5 support

Blog: WWT's ARMOR framework accelerates AI adoption with F5 support

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 made by F5, including statements regarding F5's support for and integration with WWT's AI Readiness Model for Operational Resilience (ARMOR), the expected capabilities and benefits of F5 products used in connection with the ARMOR framework, and anticipated outcomes for customers deploying AI securely across hybrid environments. These statements are based on F5's current expectations and assumptions and involve risks and uncertainties that could cause actual results to differ materially, including customer adoption, product development and integration timelines, competitive conditions, security threats, and broader market and economic factors, as well as other risks described in F5's filings with the U.S. Securities and Exchange Commission. F5 undertakes no obligation to update any forward-looking statements.

Source: F5, Inc.

View source version on businesswire.com: https://www.businesswire.com/news/home/20260303147551/en/

Jenna Becker
F5
(415) 857-2864
j.becker@f5.com

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

Source: F5, Inc.