F5 Delivers New Solutions that Radically Simplify Security for Every App and API

Apr 30, 2024 7:00 AM

- *F5 Distributed Cloud Services Web Application Scanning automates security reconnaissance and penetration testing for web applications.*
- *BIG-IP Next WAF mitigates web app and API threats while increasing operational efficiency for NetOps and SecOps teams.*
- *NGINX App Protect extends web app firewall protections for NGINX open source deployments to provide DevSecOps teams with effective controls without hindering developer agility.*

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV) today announced new best-in-class security offerings that strengthen protections and simplify management for customers. With the launches of F5 Distributed Cloud Services Web Application Scanning, BIG-IP Next Web Application Firewall (WAF), and NGINX App Protect for open source deployments, F5 is extending its leadership with the industry's most effective and most comprehensive AI-ready app and API security suite.

Many enterprises are in crisis driven by the complexity of operating hybrid and multicloud environments. According to F5's just released 2024 State of Application Strategy (SOAS) Report, 88% of enterprises are deploying apps and APIs across a mix of on-premises and cloud or edge environments. Significant time and resources are spent on continual maintenance, patching, and upgrades for physical and virtual appliances, while deployments in different clouds require unique skill sets to manage a sprawling number of tools and services. The added pressure of delivering AI-enabled services makes this crisis even worse.

F5's solutions provide high-efficacy protections with streamlined operations across distributed environments, simplifying the management and security of the exploding number of applications and APIs at the heart of modern AI-driven digital businesses. The new solutions announced today ease the burden on overwhelmed security and operations teams with consistent policy, comprehensive automation, and rich analytics.

"Modern organizations require high-efficacy app and API security that extends across their distributed environments," said Kara Sprague, EVP and Chief Product Officer at F5. "APIs are now the target of most cyberattacks, and organizations of all sizes must complement their web app security solutions with comprehensive API security. The solutions we're introducing today further enhance and extend F5's best-in-class protection for any app and any API, no matter where it is deployed."

Leading App and API Security Everywhere You Need It

F5's expansive portfolio brings the company's leading security capabilities to both traditional and modern apps and APIs—enabling customers to maintain consistent security policies across data center, cloud, and edge deployments. With a platform approach to security, F5 Distributed Cloud Services, BIG-IP, and NGINX customers can more easily combine automation capabilities with the efforts of NetOps, SecOps, DevOps, and AppDev teams to incorporate protections throughout application and API lifecycles within a CI/CD model.

With the integration of technology acquired via Heyhack to form F5 Distributed Cloud Services Web Application Scanning, customers can now access compelling automated security reconnaissance and penetration testing capabilities. Additionally, F5's award-winning Distributed Cloud Services continue to enhance API security, including the expansion of API rate limiting capabilities, improved API inventory management, JWT validation enhancements, custom pattern detection, and improved API discovery capabilities to identify zombie APIs. This approach provides greater flexibility, control, and security for API usage and management. Looking forward, F5 will deepen this integration to deliver more adaptable app and API security through automated vulnerability discovery, threat identification, and remediation.

"Advanced app and API security have never been more important, especially with the coming wave of AI-based applications and services. Simply put, F5 is the definitive leader in API security. F5's security innovations have set the standard in the market, and their holistic approach across their product portfolio has made the company a definitive leader in cloud, application, and network security," said Chris Steffen, Vice President, Research, Enterprise Management Associates. "F5 solutions bring heightened security and simplicity to increasingly complicated application security and delivery environments. We anticipate security for multicloud networking will continue to be of intense interest going forward, and F5's portfolio-driven approach offers customers effective options to guard against modern attacks in distributed environments."

F5's leadership is recognized in EMA's 2024 Vision Report, where the company's comprehensive API security solutions are lauded. Download the full report here.

Introducing Next Generation WAF for Automated Multicloud Security

Emphasizing simplicity and incorporating security throughout application development and production, BIG-IP Next brings improved security and operational efficiencies to customers of F5's flagship offering. As a prominent example, F5 BIG-IP Next WAF enhances enterprise security posture across a constantly evolving threat landscape, protecting APIs and web apps from human and bot-driven attacks. BIG-IP Next WAF can also facilitate and manage "security as code," ensuring that app and API protections can be integrated early and throughout the development pipeline. This unified approach promotes seamless transitions from testing and staging to production environments.

BIG-IP Next WAF brings added automation and an optimized cloud footprint to F5's rich BIG-IP feature set, enabling lower costs and operational simplicity. The solution enhances flexibility while maintaining consistent security policies across hybrid multicloud environments and distributed applications that rely heavily on microservices and APIs. BIG-IP Next WAF is just one module within the BIG-IP Next platform. BIG-IP Next carries forward the value proposition of reduced total cost of ownership and optimized app performance by consolidating multiple app security and delivery functions into a single in-line physical or virtual appliance. Also currently available is BIG-IP Next Local Traffic Manager (LTM), the next generation of BIG-IP LTM, with an API-centric design that reduces the complexity of managing and automating app delivery. Further security capabilities will reach the market later this year, with BIG-IP Next Access and BIG-IP Next SSL Orchestrator transitioning from limited to general availability.

"As experts in DevOps, cybersecurity, IT architecture, and compliance, we forge strong partnerships with our customers," said Grzegorz Wieczorek, CTO and Co-owner of Onito SP z.o.o. "A client, an insurance and risk management provider, required the development, security, and compliance of Kubernetes-based applications for their customers. BIG-IP Next WAF impressed with its management simplicity, API-based automation, comprehensive threat protection, and ability to rapidly deploy new policies."

Similarly, the just released version of F5 NGINX App Protect WAF on OSS further brings the power of F5's leading app security engine to Kubernetes-based applications in public clouds and on-premises deployments. With sophisticated security features and a smaller footprint, the solution separates the control and data planes, significantly reducing the corresponding attack surfaces. An ideal fit for open source and enterprise customers, version 5.0 of NGINX App Protect WAF supports both NGINX OSS and NGINX Plus and can be fully integrated into CI/CD frameworks to further enhance agile development methodologies.

Industry Insights from F5's New State of Application Strategy Report

Based on the surveyed responses of more than 700 IT decision makers from around the globe, F5 is also introducing its 2024 State of Application Strategy (SOAS) Report. Drawing from a broad mix of industries, IT leaders share their priorities and concerns with F5 in this tenth annual report highlighting digital transformation, AI ambitions, and security focal points. Data was provided by individuals in a wide range of IT and managerial roles, from the C-suite to the trenches of app development.

Additional notable findings tied to security include:

- Secure multicloud networking is a key solution for the daunting complexity of today's operations.
- The proliferation of APIs is driving changes in security practices, with 41% of organizations managing at least as many APIs as apps.
- Organizations are almost twice as likely to have automated their app and API security (43%) as their app delivery (25%).

A companion blog from Kara Sprague provides additional perspective on today's news and SOAS findings. For a contextual analysis of organizations' viewpoints tied to apps, APIs, AI, and multicloud networking, the full report is available at www.f5.com/state-of-application-strategy-report.

About F5

F5 is a multicloud application security and delivery company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure every app —on premises, in the cloud, or at the edge. F5 enables businesses to continuously stay ahead of threats while delivering exceptional, secure digital experiences for their customers. For more information, go to f5.com. (NASDAQ: FFIV)

You can also follow @F5 on X (Twitter) or visit us on LinkedIn and Facebook to learn about F5, its partners, and technologies.

F5, BIG-IP, NGINX, and other F5 product and service names are trademarks, service marks, or tradenames of F5, Inc., in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners.

Source: F5, Inc.

View source version on businesswire.com: https://www.businesswire.com/news/home/20240430306056/en/

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

Holly Lancaster
WE Communications
(415) 547-7054
hluka@we-worldwide.com

Source: F5, Inc.