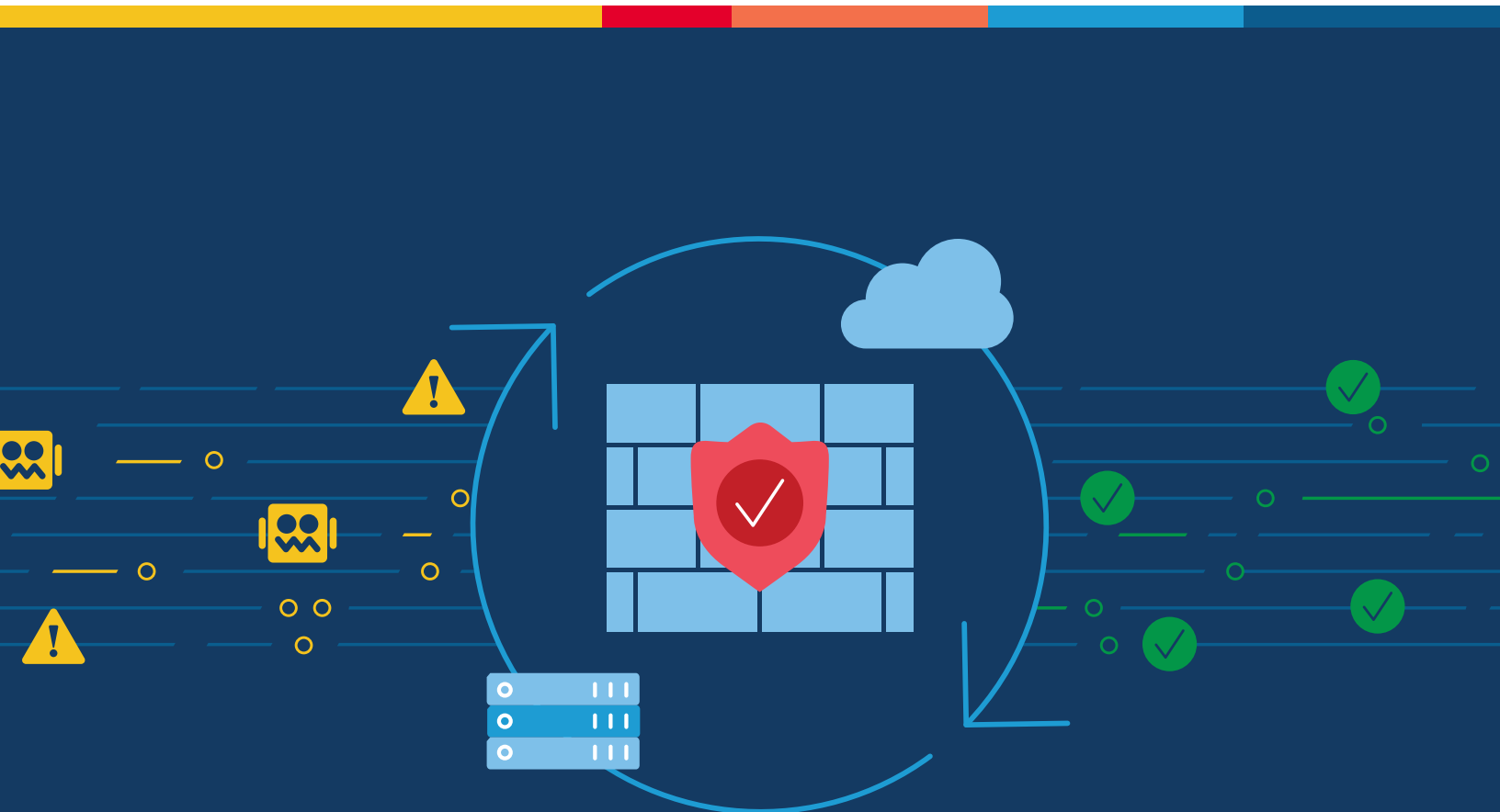




Modern Application Security for Web Apps

F5® BIG-IP® Next Web Application Firewall (WAF) protects applications in any environment—addressing web app security by keeping pace with the constantly evolving application threat landscape.



KEY BENEFITS

Improve security posture with common app attack defense

Streamlines security deployment, protecting against the most common types of attacks.

Keep protections up to date with frequent updates

Receive new security capabilities more rapidly and update modules and instances individually as available.

Migrate and apply consistent policies across all F5 WAF instances

A unified approach to WAF policies allows policies to be imported and applied consistently, from classic BIG-IP Advanced WAF to BIG-IP Next WAF, or to any F5 WAF solution.

Stop active attack campaigns

Receive security updates for the latest vulnerabilities and block current ongoing threat campaigns.

Ensure IP threat protection

Deliver contextual awareness and analysis to block threat from a dynamic set of high-risk IP addresses.

Application Security Challenges Are Constantly Evolving

With applications as the beating heart of our increasingly dispersed but hyper-connected world, information security teams face multiple challenges. The [F5 State of Application Services Report](#) found that organizations need consistency across environments, especially when it comes to security: A majority of organizations surveyed state that ensuring security and compliance in multi-cloud environments is the most challenging part of managing apps.¹ Information security teams require higher confidence when providing security parity across all application architectures and infrastructure. Given the heterogeneous mix of application architectures in the portfolios of most organizations, keeping every app secure and compliant becomes a difficult task. The latest threat research from F5 Labs found an increase in attacks on applications—creating greater security exposure.

Introducing F5 BIG-IP Next and BIG-IP Next WAF

F5® BIG-IP® Next is the evolution of F5's BIG-IP platform. It is designed to embrace modern application security challenges. Architected into separate container-based software modules, BIG-IP Next enables quicker setup, more frequent and simpler upgrading and updating, streamlined security management, easy to purchase and manage licenses, and protection for applications anywhere. This modular approach increases performance and enhances scalability, quickly adapting to evolving app security expectations.

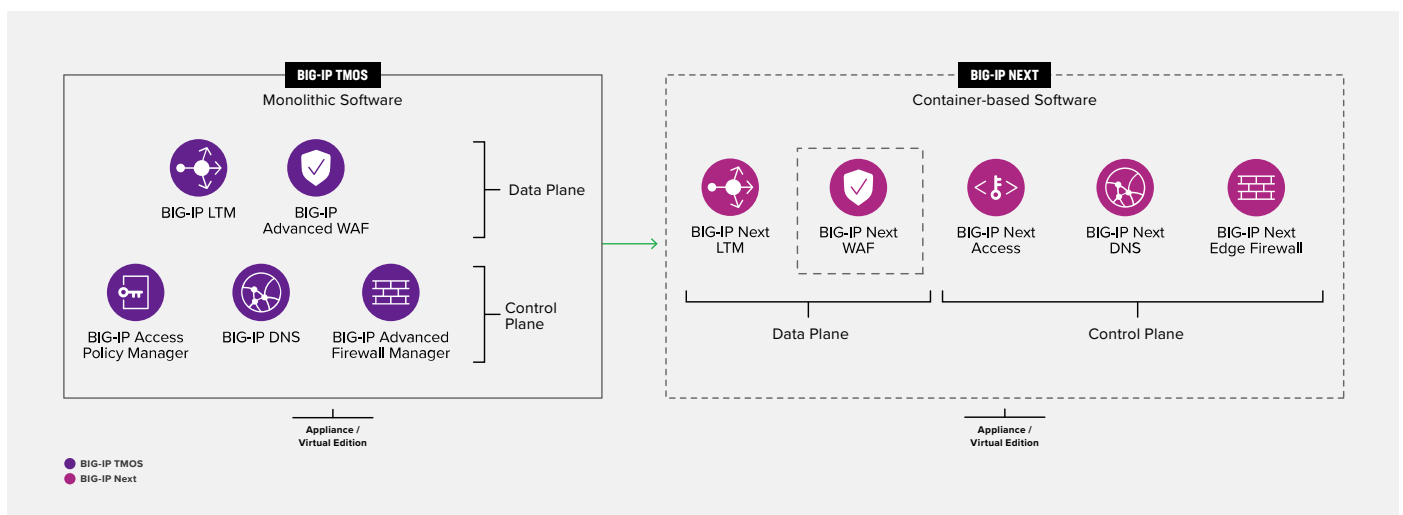


Figure 1: Container-based BIG-IP Next has a lightweight footprint.

ACCORDING TO MOST ORGANIZATIONS, ENSURING SECURITY AND COMPLIANCE IN A MULTI-CLOUD ENVIRONMENT IS THE MOST CHALLENGING PART OF MANAGING APPS.

BIG-IP Next delivers advanced app services wherever needed, whether in the public cloud, or within a data center. Its container-based software approach accelerates application delivery timeliness and allows businesses to be more agile through application programming interfaces (APIs) that are declarative and backward-compatible.

BIG-IP Next cuts cloud hosting costs by reducing footprints, lowering resource consumption, and only deploying what is necessary and used. Your administrators can simplify operations with rapid instance or module upgrades through an app-centric user interface and comprehensive cluster management capabilities. In addition, BIG-IP Next scales the scope and reach for your team—through the support of a single instance—to accommodate configuration-intensive application portfolios.

By leveraging containers in its development, BIG-IP Next also simplifies the deployment and introduction of new app security features and enhancements in a shorter time frame. Current BIG-IP customers can enjoy and apply much of the same application security that they and their mission-critical apps have grown to depend on from F5, with a platform designed for multi-cloud architectures.

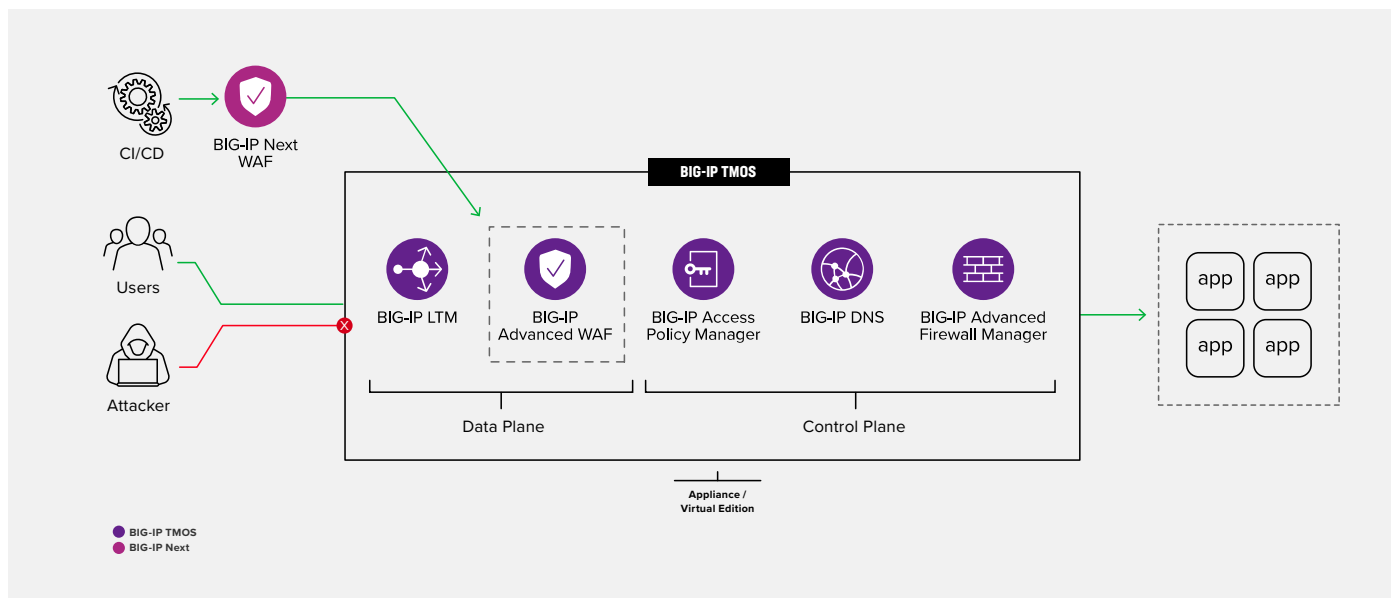


Figure 2: A simpler, more frequent upgrade and update process enhances web app and API security.

KEY FEATURES

Secures apps against common, known, and unknown (zero-day) attacks

Defends against common attack vectors, including known vulnerabilities (CVEs), OWASP Top 10, SQL/PHP injection, and more.

Mitigate layer 7 DoS

Behavioral DoS provides automatic protection against DoS attacks by analyzing behavior using machine learning (ML) and data analysis.

Enhances flexibility in protecting apps anywhere

Maintain consistent app security policies across environments—in the data center, the edge, or the public cloud.

Mitigate active attacks with F5 Threat Campaigns

Automatically mitigate active attack campaigns with intelligent updates from expert threat researchers at F5.

Defend against malicious traffic

Deliver key contextual awareness by identifying and blocking the sources of known bad IP addresses.

Protection against bot attacks

Common bot protection defends against automated threats like scanners, scraping, and malware attacks.

THE CONTAINER-BASED SOFTWARE APPROACH IN BIG-IP NEXT WAF ENABLES SECOPS TO LEVERAGE SIMPLER MANAGEMENT, FREQUENT UPGRADES, AND QUICKER SETUP TO STAY EFFORTLESSLY AHEAD OF ATTACKERS.

F5 BIG-IP Next WAF

The enhanced speed, efficiency, and simplicity enjoyed by BIG-IP Next delivers an even higher impact on modules that will run on it, including F5® BIG-IP® Next™ WAF.

Addressing ever-evolving application security challenges is a daunting task for SecOps teams. The new modular architecture of BIG-IP Next WAF allows them to receive and employ upgrades more frequently and apply updates faster, enabling them to stay ahead of the skyrocketing number and growing sophistication of exploits and threats. For instance, BIG-IP Next WAF increases the already speedy security policy setup BIG-IP customers enjoy, enabling them to defend web apps from common types of attacks, advanced threats beyond those categorized in the OWASP Top 10, unknown attacks, zero-day attacks, layer 7 DoS attacks and much more. In addition, BIG-IP Next WAF helps uncover and block current ongoing sophisticated attacks with integrated [F5 Threat Campaigns](#) and defend against malicious traffic with IP Intelligence.

The container-based software approach in BIG-IP Next WAF enables your SecOps team to leverage **simpler management, frequent upgrades, and quicker setup** to stay effortlessly ahead of attackers. The simplified management in BIG-IP Next WAF makes it easy to employ the security policy lifecycle in every phase. Frequent, streamlined upgrading enables your SecOps team to receive and deploy new features and capabilities faster, providing more seamless app protection. By releasing new security features more frequently, BIG-IP Next WAF ensures your organization will stay well ahead of new application threats and attackers.

The solution enables consistent security across environments, if required, and can maintain and update security policies similarly, whether in the data center, at the edge, or in the public cloud.

F5 BIG-IP Next WAF is designed for modern app environments as well as cloud, hybrid, and on-premises. BIG-IP Next enables automation and an optimized cloud footprint to operate WAF—with enhanced integration, streamlined security, and reduced operational costs.

Why BIG-IP Next WAF?

At the core of F5 WAFs is F5's market-leading, consistent, robust WAF engine, which is the foundation of all F5 WAFs for different delivery models—BIG-IP Advanced WAF, NGINX® App Protect WAF, F5® Distributed Cloud WAAP, as well as BIG-IP Next WAF—and will continue to be the single WAF technology stack in the future. F5's one WAF DNA enables consistency across F5 WAF offerings, including policy development, creation, and migration. It also helps simplify migration to different deployment models. Customers with dispersed, hybrid application estates can manage an application security policy in one place—no matter where their applications and WAF deployments reside. This unified policy approach is a great advantage for customers migrating from BIG-IP Advanced WAF or any F5 WAF solution to BIG-IP Next WAF.

DESIGNED FOR MULTI-CLOUD AND HYBRID ENVIRONMENTS, BIG-IP NEXT WAF ENSURES APP SECURITY AND COMPLIANCE THAT IS CONSISTENT, FAST, AND SEAMLESS.

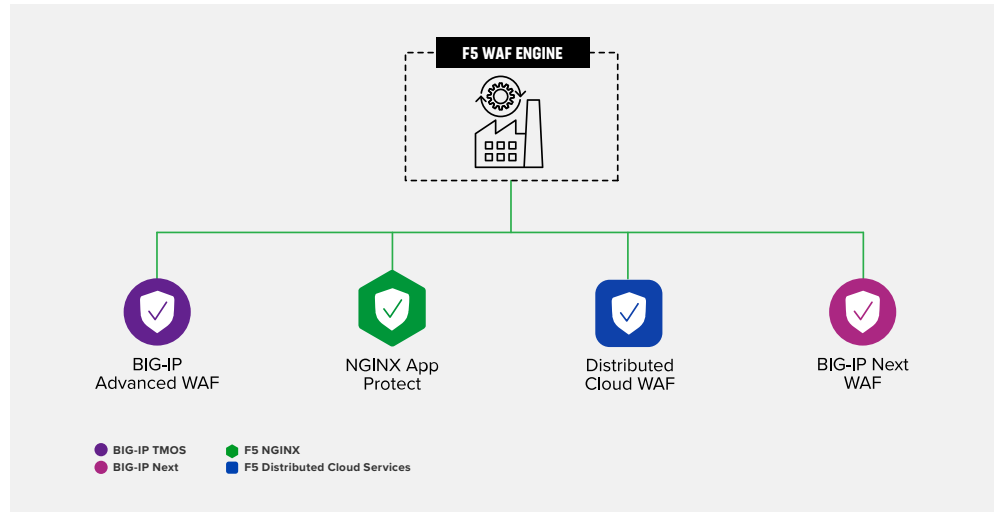


Figure 3: F5's one WAF approach makes managing a unified security policy easier.

A good number of organizations feel the most challenging task of managing apps is ensuring security and compliance. Organizations need security consistency across environments. BIG-IP Next WAF is designed for heterogeneous, multi-cloud and hybrid environments. It ensures security and compliance that is fast and seamless. BIG-IP Next WAF empowers security teams with a higher sense of confidence, enabling them to deliver consistent application security across all application architectures and infrastructures, meeting or surpassing evolving customer and business expectations for web applications.

**Find out how F5 products and solutions can help you achieve your goals.
Contact F5.**

¹ F5, Inc., 2020 State of Application Services Report, found at <https://www.f5.com/state-of-application-services-report>

