Simplify Web App and API Security with F5 and AWS

Effective security doesn't have to be complicated. Dispel common security myths and learn how to improve your security posture without complexity.

aws PARTNER

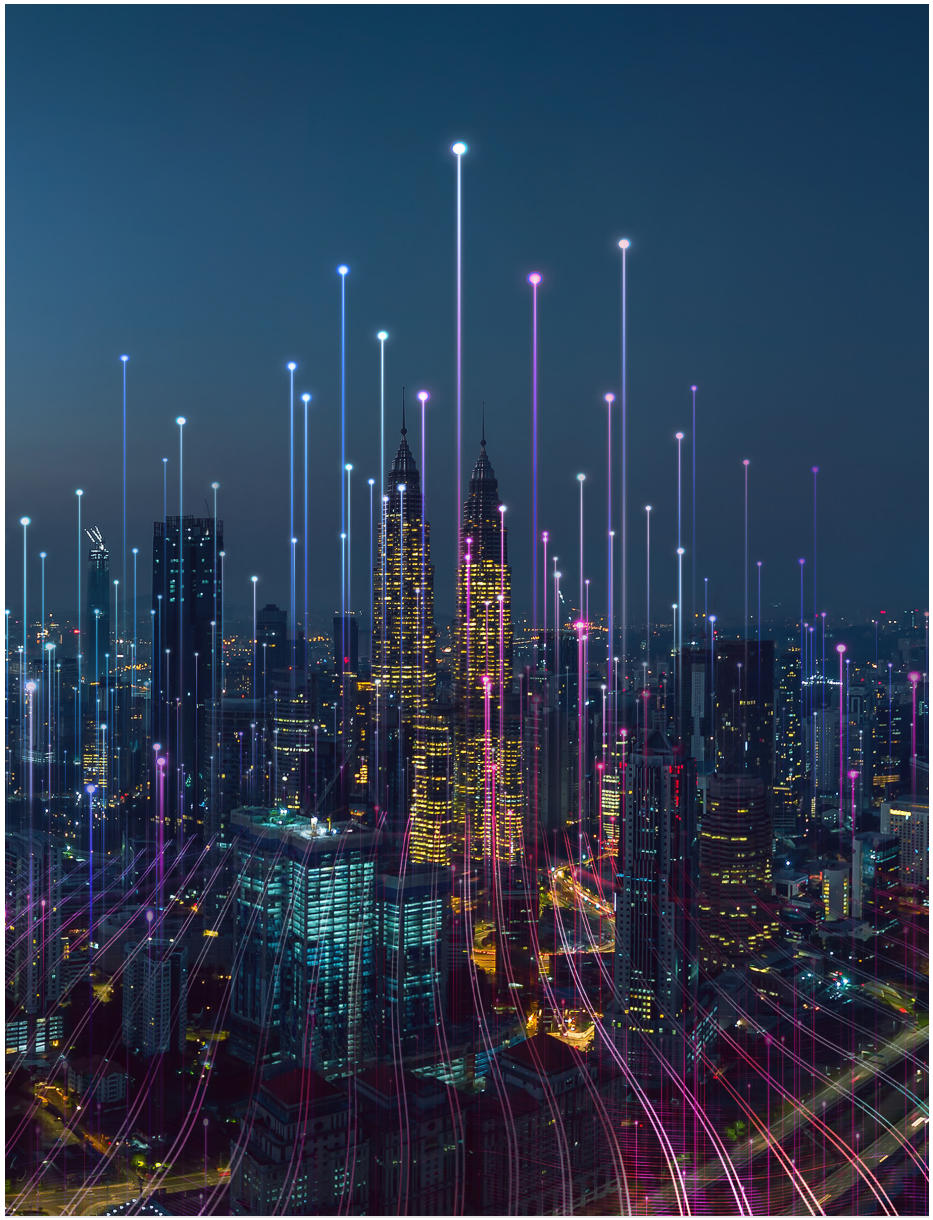
Contents

Complexity Is a Security Risk

The cybersecurity landscape has become increasingly complex as organizations struggle to manage both cloud and on-premises environments, traditional and modern apps, and the high expectations of local and global users. The explosion of web apps and APIs has further increased the attack surface. Maintaining secure and reliable operations in distributed environments while battling sophisticated threats is an uphill battle for many security and IT teams. Often these teams end up with different security tools for each environment, burdening them with more tools than they have time to manage.

This increase in complexity has also given rise to potentially harmful myths and misconceptions about app and API security. In this eBook, we'll dispel some common security myths and show how you can secure any app, any API, anywhere for reliable and cost-effective operations.

Per the Verizon Data Breach Investigations Report, basic web application attacks represented **25% of breaches**.[1]



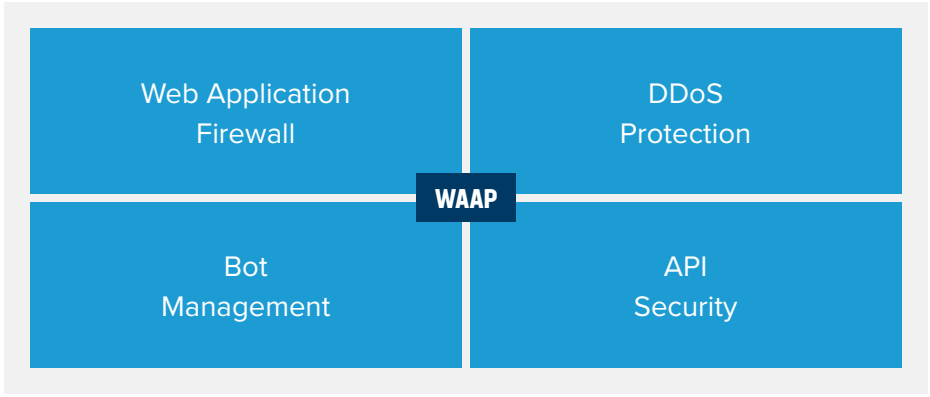
Simplify Security with Cloud-Based WAAP

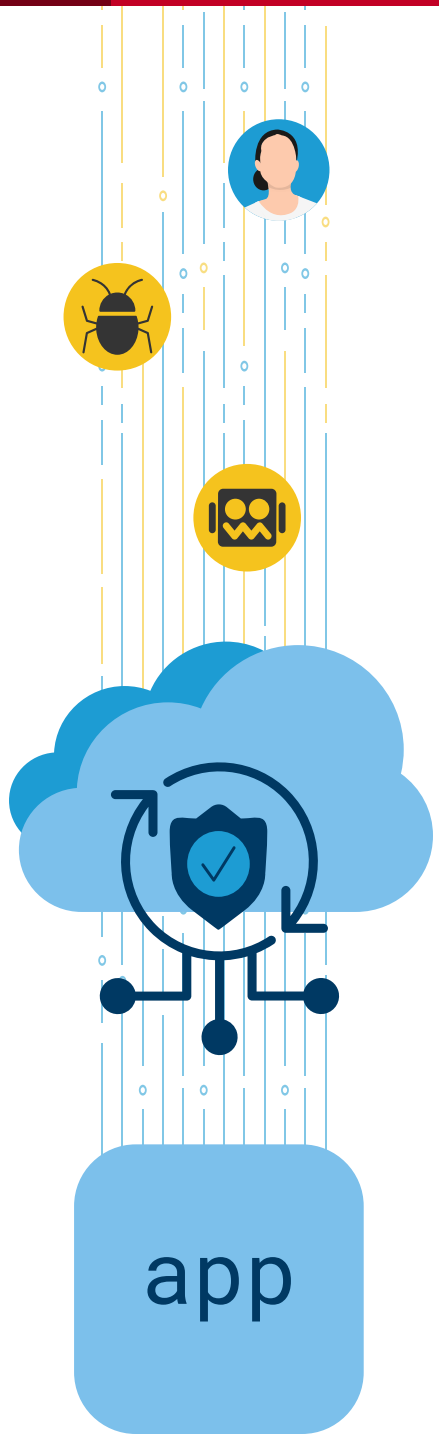
Cloud-based web application and API protection (WAAP) has emerged as an effective tool to mitigate runtime attacks like the OWASP Top 10 without adding further complexity. Simplified deployment and unified management make cloud WAAP solutions easier to deliver and manage than traditional virtual appliances, and cloud-based WAAP can protect apps and APIs anywhere: in public or private clouds, on premises, or at the edge.

WAAP enhances the native security of cloud providers like Amazon Web Services (AWS) with the added benefit of being able to use the same security platform on premises or in a private cloud. Consistent management and policies mitigate complexity in a distributed environment while improving security posture.

Four capabilities make up a cloud WAAP solution: web application firewall (WAF), distributed denial-of-service (DDoS) protection, bot management, and API security.

As an AWS partner, F5 offers F5® Distributed Cloud Web App and API Protection (WAAP) via the AWS Marketplace for easy deployment and guaranteed compatibility. Each of the four components of Distributed Cloud WAAP provide dependable security for your AWS instances so you can operate in the cloud with confidence.





Secure Apps Everywhere

The vast majority of organizations deploy apps to multiple environments. This complexity combined with the growth of modern, microservices-based applications has expanded the attack surface.

A WAF is commonly deployed to inspect traffic between apps and the Internet, allowing you to identify and block attacks such as SQL injections, cross-site scripting, L7 denial-of-service attacks, and malicious bots. However, if you use multiple WAFs in your various environments, consistency becomes a challenge.

Myth

I need separate on-premises and cloud WAFs for my hybrid environment.

Truth

A big challenge of hybrid environments is security tool proliferation, but there are cloud-based app security options that are designed to protect your apps on premises, too. This consolidation improves security consistency and reduces operational complexity.

36% of organizations say applying consistent security policies is their top multi-cloud challenge.[3]

F5 Distributed Cloud WAF, part of Distributed Cloud WAAP, protects apps across AWS, private data centers, on-premises networks, and edge clouds with unified management and consistent policies. AI and machine learning analyze behavior to accurately prioritize threats and reduce false positives.

Web app security from F5 can help you:

- Reduce time spent on managing security tools.
- Protect applications closer to the source, which can reduce strain on infrastructure.
- Accelerate time to market for secure apps with CI/CD pipeline integration.
- Remediate threats faster with real-time intelligence and continuous updates.

Protect Against Malicious Bots

Bots, whether they're beneficial or malicious, make up a significant portion of overall Internet traffic. Detecting which ones have malicious intent is a challenge, especially with rapid retooling by attackers. Adding too many hurdles for your legitimate users (including good bots) can harm your business, but unchecked bad bots can inflict serious damage, including fraud and theft.

Content delivery networks (CDNs) like Amazon CloudFront are particularly attractive targets for bot attacks. Traffic from these bad bots can significantly increase your operating costs in addition to incurring losses from fraudulent transactions.

The average business loses **$85.6 million annually** to bot attacks, up from **$33.3 million in 2020**.[4]

Effective bot defense requires a low false positive rate to reduce friction for legitimate users and beneficial bots while accurately detecting increasingly sophisticated malicious bots. It also requires the ability to outsmart attackers by employing tactics such as code obfuscation to prevent reverse engineering.

F5 Distributed Cloud Bot Defense uses human domain experts and machine learning to detect malicious bot traffic while admitting legitimate users and helpful bots. With a simple connector, you can protect CloudFront against bot attacks that include credential stuffing, fake account creation, content scraping, and inventory hoarding.

Bot defense from F5 can help you:

- Reduce costs due to bad bot activity.
- Provide better security without impacting user experience.
- Deploy defenses in the cloud easily with the pre-built connector tool.

Myth

CAPTCHA will stop bots.

Truth

CAPTCHA stops more humans than bots. Researchers found that bots solved distorted-text CAPTCHA tests correctly nearly every time. Human accuracy ranged from 50% to 84%, and humans required up to 15 seconds to solve the challenges compared to less than a second for bots.[5] In addition, user friction created by tools like CAPTCHA can lead to abandonment and lost revenue.

Discover and Secure APIs

APIs are everywhere, connecting apps and data across organizations. This explosion has expanded the attack surface in recent years, prompting OWASP to publish a Top 10 for API security. In fact, you might not even know exactly how many APIs are in your organization due to unauthorized and unmanaged shadow APIs.

Another concern are zombie APIs—forgotten, outdated, or abandoned. Without patching or maintenance, they can become an easy point of ingress for attackers. A key step to securing APIs is finding and tracking them.

According to Gartner, by 2025, **more than half of enterprise APIs** will be unmanaged.[6]

Maintain secure app integrations across hybrid or multi-cloud environments with F5 Distributed Cloud API Security, part of Distributed Cloud WAAP. Automatically discover API endpoints mapped to your applications, control connections, and monitor for anomalous behavior. F5 security on your AWS instances helps you with the shared responsibility model, as you can improve the security of your apps and data in the cloud while AWS secures infrastructure of the cloud.

API security from F5 helps you:

- Identify all API endpoints mapped to your applications via automated discovery.
- Deploy apps faster by building API security into your development processes.
- Protect APIs globally via multiple F5 points of presence.
- Increase visibility through the centralized user interface and metrics.

Myth

Developers will build in API security.

Truth

Even if your developers build in security for APIs, there are likely numerous third-party APIs operating with unknown or no security. Application security tooling may not be designed to catch all of the potential security issues in APIs, and even if an API started off with adequate security, it might not get needed updates or become a lost, unmanaged zombie API.

Mitigate DDoS Attacks

Distributed denial-of-service (DDoS) attacks have escalated in scale and sophistication, with peak bandwidth up 216% since 2020.[7] Attackers now leverage virtual private servers to create massive, high-performance botnets that overwhelm defenses and even extort ransoms from victims.

Modern DDoS attacks are now largely at the application layer (L7), but an effective solution should defend L3-L7 to also protect against volumetric and multi-vector attacks.

Application layer DDoS attacks are **up by 165%**.[8]

Multi-layered DDoS protection from F5 and AWS keeps your applications secure and available to support your business. AWS provides secure and resilient services with several forms of DDoS mitigation built in. F5 Distributed Cloud DDoS Mitigation, part of Distributed Cloud WAAP, protects against L3-L7 attacks in every environment, including AWS.

DDoS mitigation from F5 can help you:

- Maintain business continuity by stopping attacks before they impact your network and applications.
- Increase operational efficiency by reducing the time spent to respond to attacks manually.
- Gain visibility and insights via a centralized console and reporting.
- Reduce operating costs by blocking malicious traffic that increases your bandwidth usage and infrastructure costs.
- Scale dynamically and deploy new services without the need for additional appliances or network capacity.

Myth

Distributed architectures are immune to DDoS attacks.

Truth

Modern multi-cloud environments, CDNs, and distributed app architectures can reduce the impact of volumetric attacks, but without a DDoS mitigation solution, you're still at risk of performance degradation, outages, or increased costs. The massive scale of sophisticated botnets can overwhelm distributed environments.

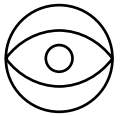
F5 and AWS Offer Security Without Complexity

With a partnership spanning over 10 years and 25,000 customers, F5 and AWS can provide you with the right tools for secure and high-performing apps at scale. F5 holds three AWS competencies for security, containers, and networking, as well as multiple service validations (CloudFront, Linux, Outpost, AWS WAF) and service reference architectures (EKS, AGA, GWLB, Local Zones). This ensures seamless security and interoperability for your AWS services.

The SaaS-based platform of F5 Distributed Cloud WAAP provides consistent protection for applications and APIs across every environment with unified management to provide:

Comprehensive protection

Simpler operations



End-to-end observability

Simplify your path to effective security without sacrificing user experience or innovation speed. Learn how F5 Distributed Cloud WAAP can simplify effective security for your apps on AWS and everywhere else.

[1] Verizon, 2023 Data Breach Investigations Report, June 2023

[2] Gartner, Hype Cycle for Application Security, July 2023

[3] F5, 2023 State of Application Strategy Report

[4] Infosecurity Magazine, Bot Attack Costs Double to $86m Annually, September 2023

[5] Andrew Searles, et al., An Empirical Study & Evaluation of Modern CAPTCHAs, UC Irvine, July 2023

[6] Gartner, Predicts 2022: APIs Demand Improved Security and Management

[7] F5 Labs, 2023 DDoS Attack Trends, February 2023

[8] F5 Labs, 2023 DDoS Attack Trends, February 2023

ABOUT F5

F5 is a multi-cloud application services and security 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 providing exceptional, secure digital experiences for their customers.

Visit f5.com/cloud/use-cases/web-application-and-api-protection-waap