SECURING WEB APPLICATIONS IN CONTAINER-BASED ENVIRONMENTS

EXECUTIVE SUMMARY

A lack of dynamic security capabilities that can keep pace with the ever-changing nature of DevOps environments leaves organizations exposed to risks from advanced malware and other sophisticated forms of attack. This vulnerability applies to containerization tools that allow applications to be packaged and moved from one development environment to another. Traditional web application firewalls cannot provide adequate protection under these conditions. But the Fortinet FortiWeb Web Application Firewall Container Edition is designed to protect web-based applications and internet-facing data from threats within container-based environments.

RETHINKING APPLICATION DEVELOPMENT AND DELIVERY

Traditional software development blends a range of features and services (e.g., databases, web servers, application code) into a single, highly integrated package. But in today’s responsive and consumer-driven digital marketplace, this monolithic approach to development and deployment can severely slow down an organization’s ability to respond to business and market demands.

In response, business unit software architects are employing new microservices architectures and container-based environments to help accelerate application development and delivery. In contrast to traditional, highly integrated approaches of software and network architecture development, these more agile approaches build each component and feature autonomously, independent of other functions. They typically leverage open communications standards or orchestration systems for the different components to interoperate. This iterative, incremental methodology allows organizations to develop, deliver, and customize their applications, software, and infrastructures more rapidly. This, in turn, enables them to more effectively respond to the continually evolving demands of modern digital environments.

FASTER PROCESSES BRING NEW SECURITY CHALLENGES

Speed and agility are important—but not at the expense of security. In establishing a faster and more efficient development operations (DevOps) methodology, it can be easy to overlook opening a back door or creating an inadvertent security vulnerability in the process. Code checks and user acceptance testing (UAT) can help catch obvious issues. However, it is nearly impossible to address every possible vulnerability in custom code.

Even with a traditional web application firewall (WAF) in place, problems remain. Protocols and operations in DevOps constantly change and can make WAF configuration irrelevant, which must then be manually reconfigured. These manual processes create additional security overhead and opportunities for errors. Even if it were possible to address every issue and manually reconfigure security measures, the time it takes to do so increases costs and slows processes to a crawl.

PACKAGING FOR PORTABILITY PLUS SCALABILITY

Containerization tools (such as Docker) allow an entire application to be bundled together so that it can be moved seamlessly from environment to environment. This can be done from a developer’s laptop to a test environment, from a staging environment to production, and even from a physical machine deployed in a data center to a virtual machine located in a private or public cloud. This significantly simplifies deployment, management, updates, and interoperability.

As part of containerization, all application elements (including databases, code libraries, supporting applications) are placed together into a bundle of separate containers that work together to compose the application. This is commonly known as a pod or service composition. In this instance, everything for the application is ready to go—with the exception of application security.

DEVOPS, DOCKER, AND DOUBT

- 25% of companies have adopted the Docker containerization platform for DevOps.¹
- 81% of CISOs are concerned with risks related to DevOps that allow vulnerabilities to slip in along with the faster pace of development.²
Running a container environment for web-based applications typically includes an orchestration tool (such as Kubernetes). As needs grow, the orchestration platform automatically expands (scales out) or contracts (scales in) the application environment to accommodate demand—increases and decreases. Adding a container-based WAF to an orchestrated environment enables security to scale alongside applications as they adjust dynamically.

FORTIWEB WEB APPLICATION FIREWALL CONTAINER EDITION

FortiWeb WAFs provide artificial intelligence (AI)-enhanced and layered web application threat protection for midsize businesses and large enterprises, application service providers, and Software-as-a-Service (SaaS) providers. They are designed to protect web-based applications and internet-facing data from attacks and breaches. Using advanced techniques, it provides bidirectional protection against malicious sources, distributed denial-of-service (DDoS) attacks, and sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, file inclusion, and cookie poisoning attacks.

The FortiWeb Container Edition primarily targets container-based environments that support Docker in numerous platforms. This includes private/public registries, Docker Enterprise, and Amazon Elastic Container Service (ECS).

**FIGURE 1: MICROSERVICES ARCHITECTURE**

OUT-OF-THE-BOX SECURITY FOR CONTAINERIZED DEVOPS

As organizations adopt more agile development strategies, security will continue to be a critical consideration. When a development team writes, tests, updates, or deploys an application using a containerized microservices architecture, the environment remains consistent across all parts of the application life cycle. This makes collaboration between different teams (developers, testers, and administrators) easier because they all are working within the same containerized environment. FortiWeb’s container-based WAF provides security that moves with an application wherever it is hosted while scaling as needed with demand.

The FortiWeb Container Edition is available from Fortinet Reseller Partners. AWS customers can also deploy the FortiWeb Container Edition with an advance license purchase.

---


---

www.fortinet.com