Enterprise-Grade Application Security and Visibility in an OpenShift Container Platform

Comprehensive container security requires both visibility at layer 7 and security at the enterprise level. These capabilities each play a role in protecting north-south traffic (client-to-server, between the data center and the rest of the world) and east-west traffic (machine-to-machine inside the OpenShift cluster).

F5 solutions, combined with the open-source ELK stack and Red Hat Ansible, deliver important security capabilities and benefits for your containerized applications, including protection at both the application and enterprise levels. These capabilities include:

KEY BENEFITS

Multi-layered application security
Deploy highly scalable controls against web application attacks with security for apps that run as microservices in a container environment.

Layer 7 visibility
Gain network visibility for application transactions in OpenShift and monitor those transactions and security alerts from a single ELK stack dashboard.

Faster response times
Reduce the time an attacker has network access and minimize risk when you can respond immediately.

Security from inside threats
Protect critical applications from lateral attacks and secure traffic between cluster containers.

Multi-layered application security

- F5® Advanced WAF provides highly scalable, common controls against web application attacks, including those in the OWASP Top 10.
- F5® Essential App Protect Cloud Service, powered by NGINX, improves security for apps that run as microservices in a container environment.

Layer 7 visibility

- Gain network visibility for all application transactions in OpenShift.
- Use a single ELK stack dashboard to monitor all your application transactions and security alerts.

Faster response times

- Reduce the number of days an attacker has access to a network before being discovered. (The current median is 56 days, according to FireEye Mandiant.)
- Minimize risk with immediate incident response.

Security from inside threats

- Protect critical applications from lateral attacks between applications in different namespaces.
- Secure traffic between containers within the same OpenShift cluster.

Layered Security Policy for North-South Traffic

Web application security is important for most enterprises, even those that don't consider themselves web-based businesses. The global, open nature of the Internet exposes organizations to attack from any location, and the scale and complexity of these attacks can be overwhelming. F5 helps protect your OpenShift-based applications and data from outside threats with high efficacy security controls that block general threats before they infiltrate your network and institute application-specific policies that defeat targeted threats before they can misuse your apps.

AS APPS MOVE TO CONTAINER DEPLOYMENTS, SO TOO DO THE THREATS—AND SO DO THE APPLICATIONS AND SERVICES THAT PROTECT AGAINST THOSE THREATS.

The first line of defense is the F5 Advanced WAF. Advanced WAF is configured to enforce common security controls across all enterprise applications. These controls provide protections against application and platform vulnerabilities and the OWASP Top 10, including injections, scripting, and server-side request forgery.

F5 Advanced WAF inspects all incoming traffic against those policy definitions and others. When it recognizes an attempt to infiltrate your application using any of these tactics, Advanced WAF immediately blocks that traffic.

The second line of defense is F5 Essential App Protect Cloud Service, (also known as NGNIX App Protect), a modern app security solution that works seamlessly in DevOps environments to protect applications. This solution is built on F5's market-leading security expertise. NGINX App Protect makes security pain-free with a security-as-code philosophy that integrates easily into DevOps pipelines, where its declarative configuration capabilities make it easy to automate application security and testing.

Web application firewall (WAF) protection and authentication are provisioned with different Kubernetes objects (or custom resources) and comply with Kubernetes RBAC practices. Therefore, you can securely delegate WAF configuration to a dedicated DevSecOps team, while delegating the authentication and load balancing configuration to a DevOps team or app owners. Because security and authentication are so close to the backend apps, you get dynamic security that's integrated with the development lifecycle of your containerized apps.

Throughout this process, both Advanced WAF and NGINX App Protect are continually exporting detailed data (network telemetry from Advanced WAF, alert data from NGINX App Protect) into Elasticsearch, which maintains a centralized pool to monitor all your network and apps. This automated process is significantly more efficient than the traditional process of manually managing hundreds of point solutions. It can also trigger additional actions: If any of the data meet conditions defined by the user (for example, it originates from a denylisted IP address or region), ELK Watcher will execute the appropriate Ansible playbook. Ansible playbooks can be programmed for any number of tasks, including updating Advanced WAF profiles to block previously unidentified threats.

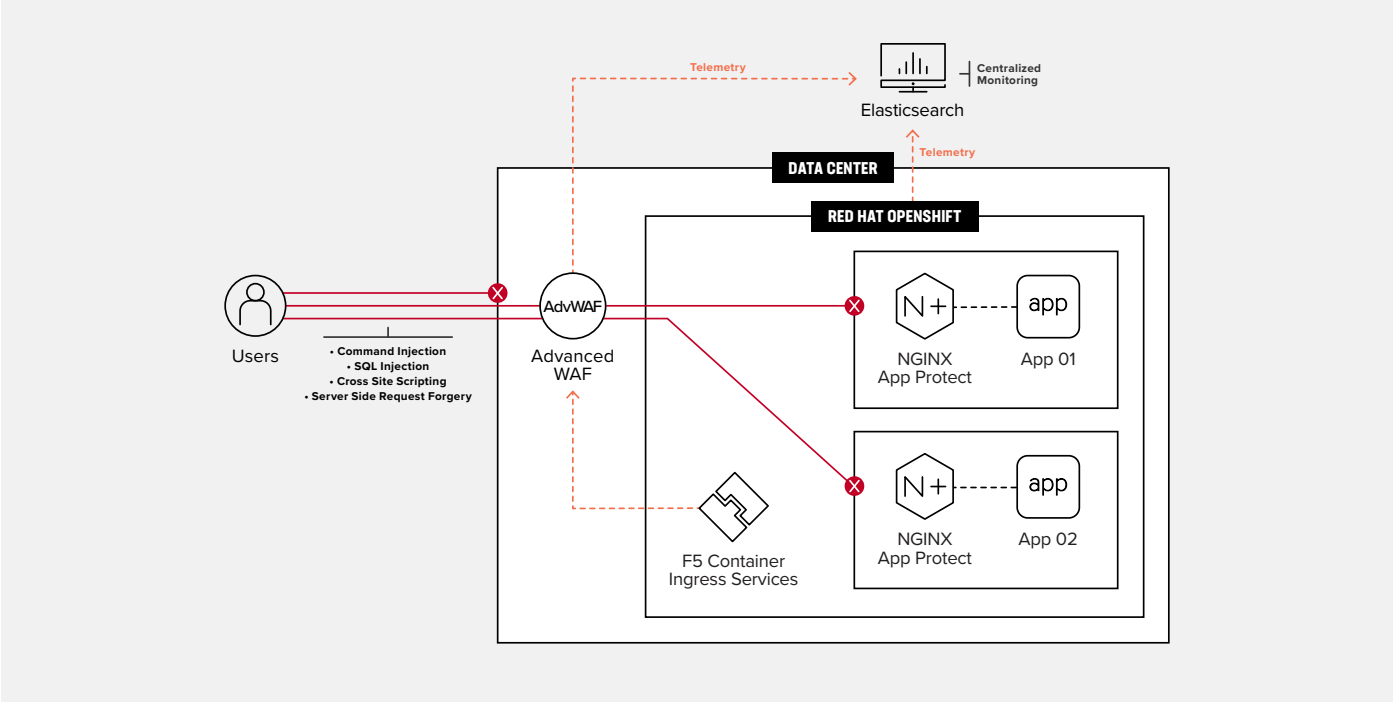

Figure 1: F5 Advanced WAF and NGINX App Protect work together to block unwanted traffic and protect your dev environment.

For organizations that prefer an as-a-service model for application security in containers, the role of Advanced WAF in the above example can be accomplished by the F5® Essential App Protect Cloud Services or the F5® Silverline® Managed Security Service.

Protecting Critical Apps Against East-West Attacks

There are so many ways for an attacker to try to assault your containerized applications, Microsoft created a wide-reaching attack matrix to track the biggest offenders. The matrix includes lateral attacks where attackers gain access to one container, use that to access resources within the cluster, and then use those resources to gain access to the underlying node or even to the cloud environment.

An example of one such malware-based attack takes advantage of developer test environments to sneak its way into enterprise systems. It typically looks something like this:

1. The attacker gains initial access via a phishing email and obtains the user ID from the compromised laptop.
2. The attacker uses that stolen ID to infiltrate software under development in a dev namespace.
3. From within the dev space, the malware executes its primary web attack, targeting the live version of the app. Mayhem ensues.

While this is by no means the only way to execute a lateral attack, it does illustrate the need for security measures within your container environments, not just at the front door. As before, automated threat remediation is enabled by NGNIX App Protect, Elasticsearch, and Ansible:

- NGNIX App Protect monitors all web requests for the application servers.
- NGNIX App Protect exports the alert details to the external Elasticsearch system.
- If any of the predefined alert conditions are met, ELK Watcher will execute the already configured Ansible playbook.
- The Ansible playbook deletes the tainted pod from the OpenShift container.

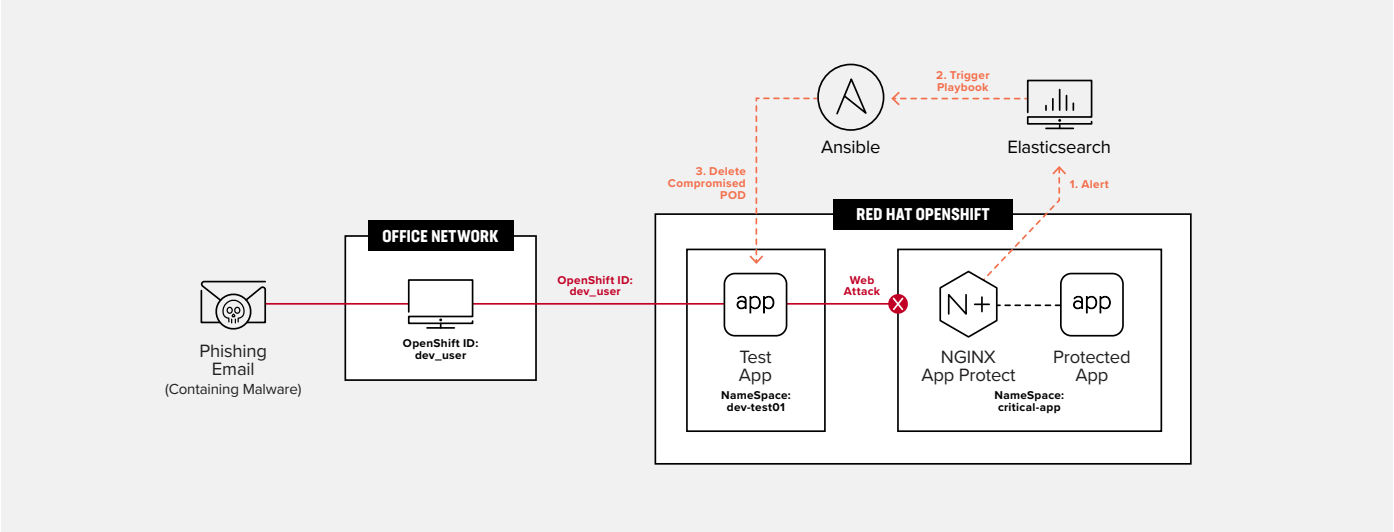

Figure 2: NGNIX App Protect, Elasticsearch, and Ansible can be tightly integrated to deliver powerful, automated threat remediation.

F5 PRODUCTS

F5 Advanced WAF

NGINX App Protect

F5 Essential App Protect Cloud Services

F5 Silverline Managed Security Services

Summary

To meet the twin goals of minimizing risk and maximizing uptime, networking pros have historically prioritized control over speed and innovation. This can put them at odds with DevOps, which is typically focused on producing the next new thing and prioritizes the ability to react quickly and iterate constantly. Unfortunately, if DevOps and NetOps are not in harmony, security suffers. As a result, attackers have learned to probe dev networks and app deployment infrastructures to identify and target weak spots.

As apps move to container deployments, so too do the threats—and so do the applications and services that protect against those threats. F5 offers comprehensive container security solutions that deliver layer 7 visibility and enterprise-level security. F5 Advanced WAF and NGNIX App Protect work closely with leading open source solutions to defend against the full range of attacks, from outside the data center and from within.

For more information, visit F5.com for the resources below.

Solution Area

Prevent Downtime and Breaches by Securing Your Modern Apps and APIs

Use Case

Ansible Automation for F5 Solutions and Use Cases

Blog

F5 AS3 and Red Hat Ansible Automation

Partner Information

Certified Integration: Ansible and F5