Add Security to Your Amazon EKS

Protect your applications with NGINX Plus and NGINX Ingress Controller.

In collaboration with

Mitigate OWASP threats and beyond

Keeping applications secure can be one of the most daunting—and critical—challenges for any enterprise to figure out. Major breaches like SolarWinds and Colonial Pipeline have shown that companies need to devote more and more resources to thwart bad actors.

Attempts to breach security happen thousands of times a day. Yet only 5 percent of apps in a company's portfolio are protected.[1] In the last decade or so, there's been a transformation in app development. Over 50 percent of organizations claim they simply couldn't operate without apps. And 67 percent think that digital efforts like IT and business process optimization accelerate the release of new products and services.[2]

But the speed at which applications are now developed comes with a challenge: How can security teams keep up with the need to check apps when developers outnumber security pros 500 to 1?[3]

In this eBook, discover how you can prevent security breaches with NGINX, part of F5, and Amazon Web Services (AWS). Learn how to protect your apps in an Amazon Elastic Kubernetes Service (Amazon EKS) deployment from a range of threats, including the Open Web Application Security Project (OWASP) Top 10 and beyond.

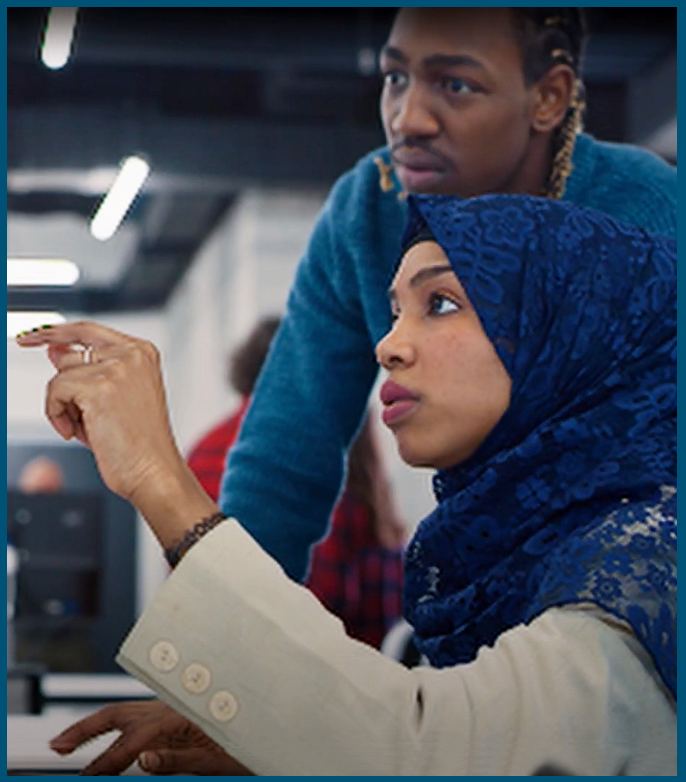

Figure 1. F5 NGINX Controller Overview: Faster deployments, fewer headaches.

[1] 2019 Varonis Global Data Risk Report
[2] F5 2021 State of Application Strategy Report
[3] The Daily Swig, GitHub's Nico Waisman: 'Security is not just an opportunity, but a responsibility for us,' June 2020

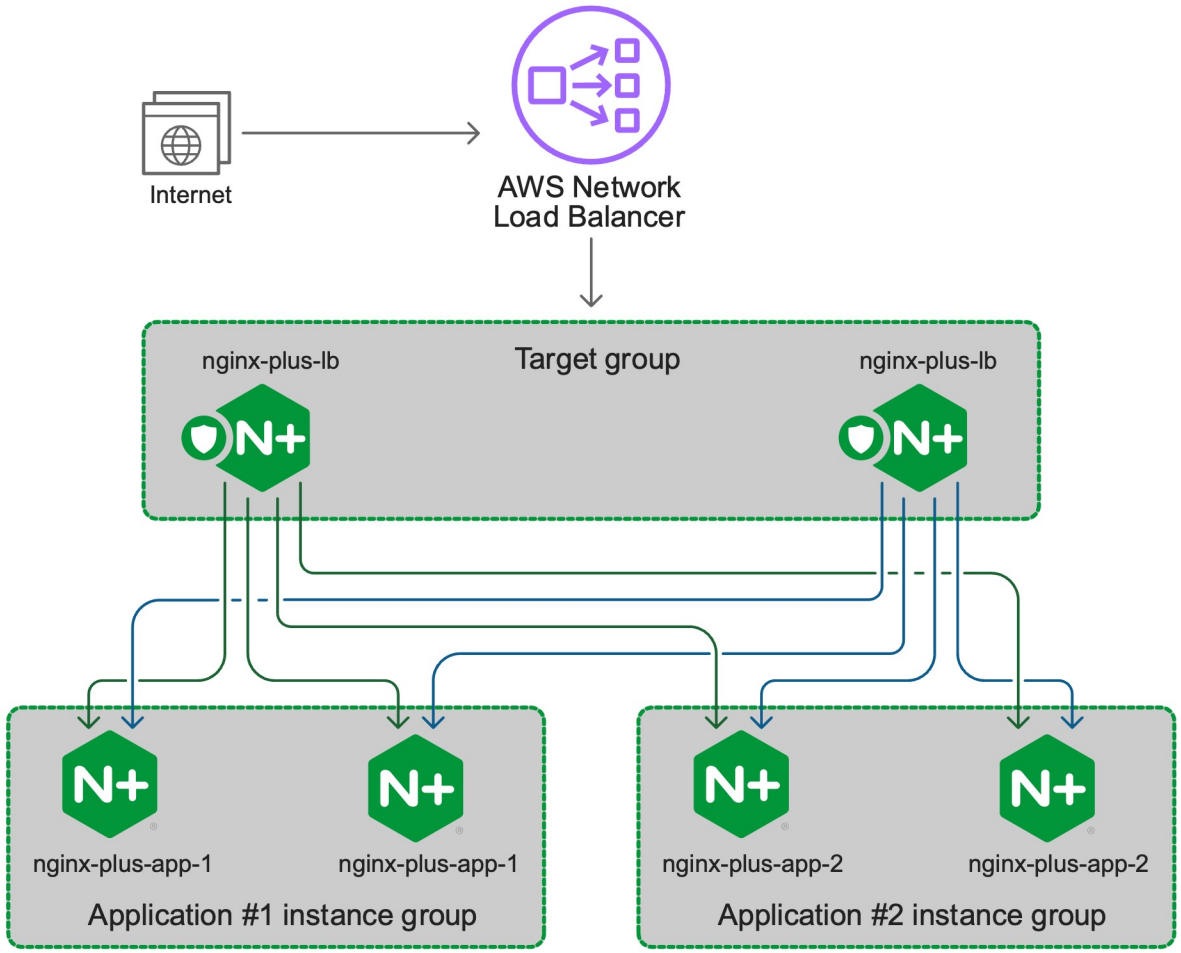

Figure 2. NGINX App Protect easily integrates with NGINX Ingress Controller and NGINX Plus, creating greater security for your apps.

How can NGINX help?

NGINX is a security solution for modern apps that offers different options:

- **NGINX Ingress Controller** is a traffic management solution for cloud-native apps in Kubernetes and containerized environments.
- **NGINX Plus** is a cloud-native, easy-to-use reverse proxy, load balancer, and API gateway.
- **NGINX App Protect** works in DevOps environments as a robust web application firewall (WAF) or app-level DoS defense.

Secure your apps in Kubernetes

Security tools such as WAFs are used to protect applications from outside attacks. SecOps has typically deployed them integrated with a load balancer at the network edge (or front door), creating a secure perimeter.

However, security breaches of modern apps have shown that crucial refinements to this approach are necessary:

First, securing the perimeter is not enough. It's rare that there is a single perimeter that's easy to secure, so proxy-based security tools such as WAFs need to be closer to the apps they are protecting.

Second, security matters now involve more than the chief information security officer (CISO) and SecOps team. It spans the entire organization. DevOps plays a critical role as well by accepting, testing, and deploying security policies in its CI/CD pipeline.

Open Web Application Security Project (OWASP) automated threats to web applications:

- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery (SSRF)

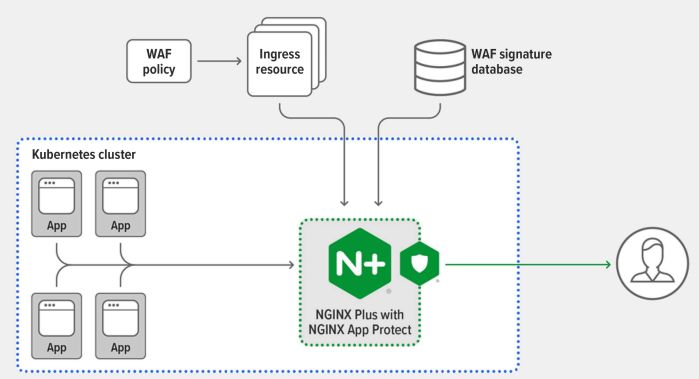

Figure 3. NGINX secures the app perimeter while consolidating the data plane and the control plane.

Five ways to mitigate vulnerabilities faster and easier

Tracking vulnerabilities and sophisticated attacks against applications and infrastructure—and mitigating them—can be tedious and time consuming. Application teams need to focus on delivering code, not worrying over security matters. NGINX Plus helps relieve those concerns with five specific ways of resolving vulnerabilities faster and easier for subscribers:

1. **Up-to-date info:** Upon the release of a security patch, NGINX Plus subscribers hear about it through timely and direct email updates, rather than having to independently monitor databases and blogs.

2. **Real-time help:** F5 customers under attack (including NGINX Plus subscribers) have access to the F5 Security Incident Response Team (SIRT), which helps get you back up and running quickly while looking ahead to anticipate and deter future threats.

3. **Enhanced app protection:** With NGINX App Protect, an enterprise-grade WAF, subscribers don't have to build their own signatures and deal with multiple false positives.

4. **Sophisticated authentication protocols:** With authentication based on JSON Web Token (JWT) and OpenID Connect—for web and API clients—NGINX Plus goes beyond the methods in NGINX Open Source to deter bad actors from accessing your applications and infrastructure.

5. **Timely patches:** If a vulnerability is found affecting NGINIX software, advanced warning allows more time to develop a patch before the issue is publicly disclosed and before bad actors can exploit it. That fix is available to NGINX customers as patched binaries.

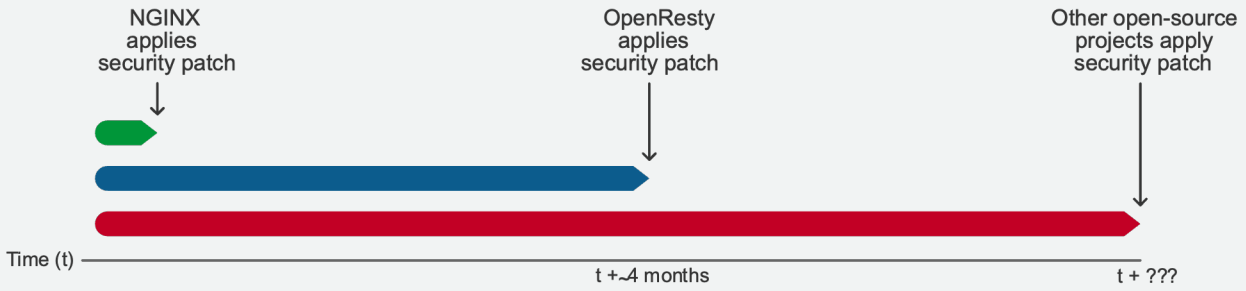

Figure 4. Example of advanced warning and timely patches.

Customer case study: Zipwhip

Zipwhip, a text messaging provider, was facing 280 percent growth across its platform and trying to find a security solution that could keep up with its success. The company looked into hardware solutions, but the costs and timelines were not feasible. So, it moved everything out of its colocations to the AWS Cloud, supported by F5 and NGINX security solutions.

"We were literally holding up half the company with one hand as we were trying to move to the next gen of everything on the other hand," says Kolby Allen, Platform Operations Architect at Zipwhip. "And AWS was really the reason we were able to achieve it."

Zipwhip uses NGINX for many of its Kubernetes clusters. And F5 sits on the internal edge between its AWS network and colocations.

"AWS has provided the infrastructure for us … the performance that we need," says Allen. "On top of that, F5 has been as performant. We were able to drop that in and it was able to keep up with the underlying [Amazon Elastic Compute Cloud (Amazon EC2)] speeds … and has provided the same visibility for us across the board."

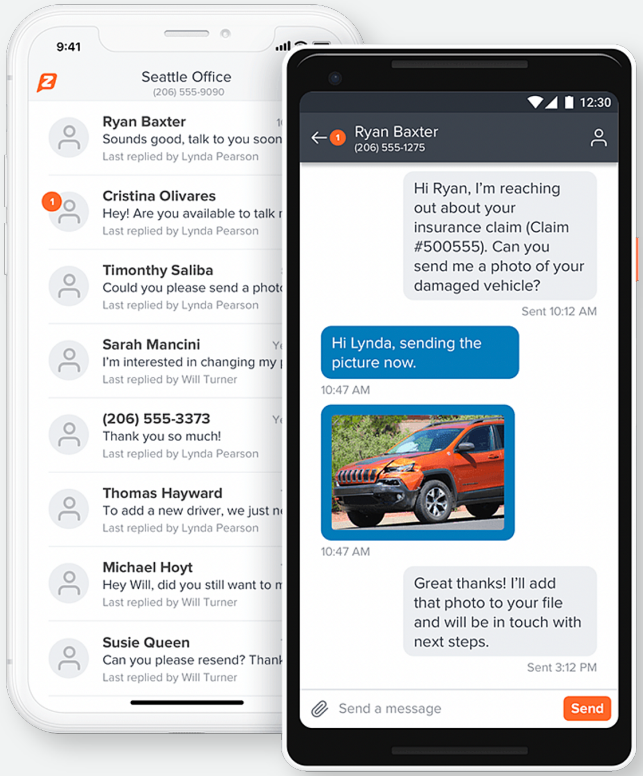

Figure 5. Image of separate business and personal text messages. Zipwhip's Android and iOS apps allow you to text from your landline or toll-free phone number on your smartphone and tablet when you're on the go.

NGINX Plus and NGINX Ingress Controller in AWS Marketplace

F5, Inc., the company behind popular open-source project NGINX, offers a suite of technologies for developing and delivering modern apps. The F5 portfolio of automation, security, performance, and insight capabilities empowers AWS customers to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users.

NGINX and F5 solutions bring NetOps and DevOps closer together, with app services spanning from code to customer.

Directly purchase the NGINX Plus-based version of NGINX Ingress Controller, with and without NGINX App Protect, in **AWS Marketplace for Containers**.

- Networking Competency
- Security Software Competency