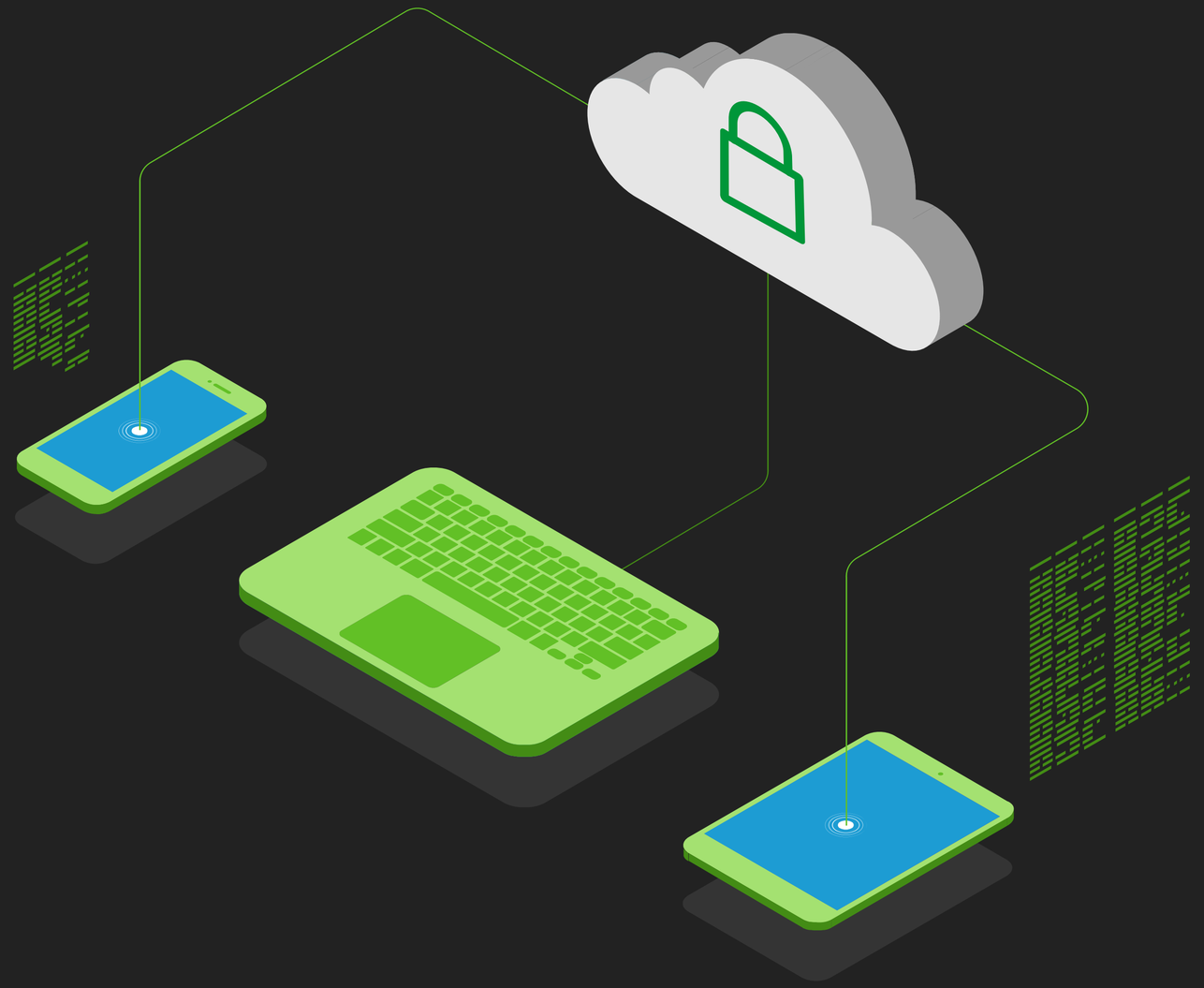
NGINX App Protect®
Web Application Firewall



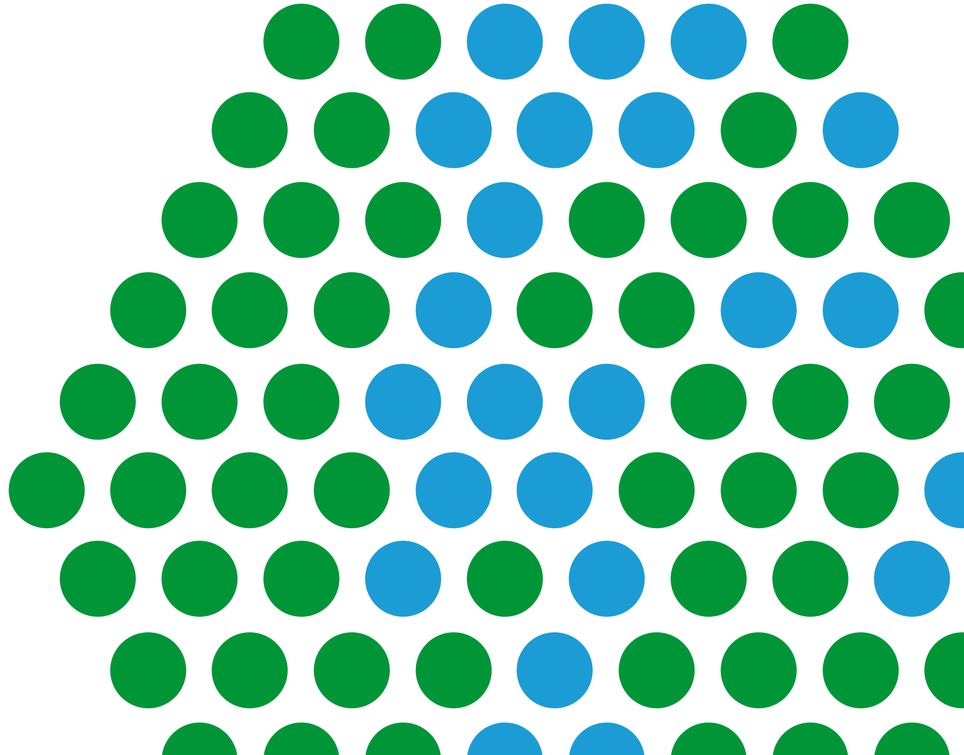
The Secret to Modern Application Security

How F5 NGINX App Protect WAF Can Help Your Organization Prevent Downtime and Data Breaches by Securing Your Apps and APIs

NGINX is a part of F5

CONTENTS

NGINX App Protect
Web Application Firewall



Being agile is something every business strives for: adapting quickly to the latest trends, keeping up with competitors, and better serving your customers and employees, are all more essential than ever before. And in today's business world, it means doing it faster than ever before.

The way to do that is through modern applications and APIs, and a lot of companies are already using them.

In fact, 85% of new workloads are deployed in containers and 83% of internet traffic is made up of API calls.[3]

An agile company uses microservices architecture to operate at the pace of modern business and harnesses DevOps to rapidly design, deploy, and redefine applications. The speed of this agile software development, characterized by continuous integration and deployment, is rooted in a heavy reliance on automation. Adaptive applications of this nature are built to be redefined quickly and frequently so that business innovation can be delivered at a pace that matches the market. Such speed ensures customers are served quickly and can enjoy high quality experiences when accessing a company's services, reducing barriers to purchase while increasing loyalty.

In a business market that gets more competitive every day, it's all too easy for a customer or potential client to look elsewhere if an app or website doesn't provide them with a positive experience. That's why modern application development methods are so popular – but they also have a downside when it comes to security.

Performance Matters

Google research has found that customer expectations are rising dramatically and that customers will quickly look elsewhere if they receive a less than optimal experience from an online service.

For example, **a page load time of one to three seconds** increases the probability of a person leaving a site by

32%.

One to five seconds delay has a

90%

bounce likelihood.[1]

Elsewhere,

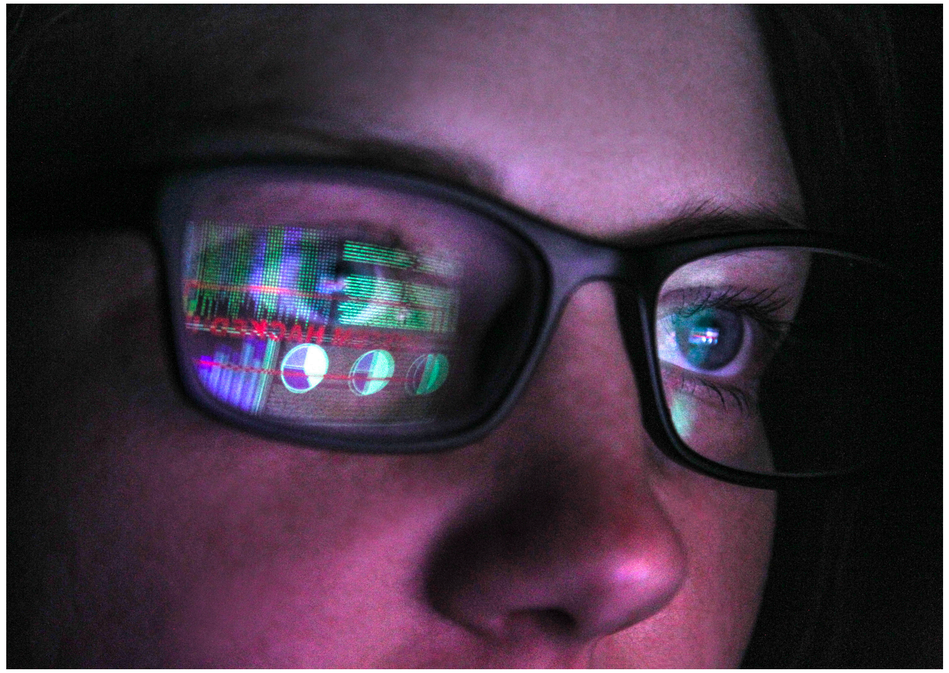
53%

of mobile website visitors will leave if a webpage **doesn't load within three seconds.**[2]

This is crucial information for businesses. The performance of your applications directly impacts customer experience and sales.

SECURITY BOTTLENECKS MEAN FRICTION

Traditional application development saw security teams apply their policies and carry out checks at the end of the process. But today's pace of deployment makes it impossible for them to keep up. To take an extreme example from back in 2015: **Amazon hit 50 million production deployments in a year**.[4] That's about one deployment per second. How can traditional SecOps practices possibly hope to keep such a frantic pace? That leaves businesses with a tough decision to make: slow down development in the modern environments they've invested heavily in to ensure adequate protection for their apps, or continue at speed, cutting corners on security? Given the current threat landscape, the latter can pose a significant risk.



What worries developers most?*

Security
50%

Availability & Reliability
39%

System Failure
39%

Performance
34%

Scalability
27%

Complexity
24%

Automation
23%

Source: NGINX, The State of Modern App Delivery 2020

*Respondents could choose multiple options.

Every day, over 30,000 websites are hacked – an attack is launched every 39 seconds.[5] These aren't just attacks on code, either. **Over 20% of data breaches discovered during the last year occurred due to code errors, and over 40% of those attacks targeted web applications.**[6] And with the decentralized nature of modern applications providing a far larger attack surface, any weak point within an application stack is now a potential risk. With apps and their associated microservices reaching out to more and more locations, even to those of third parties, hackers have more avenues of opportunity and positions from which to strike. Unlike the early days of the internet when a castle-and-moat approach was effective for keeping bad guys out of an internal network, the new front-line is the modern application – the point where the network meets a user. Any user. And those users may not always have good intentions.

TRADITION VS. TRANSFORMATION

The root of the problem is conflicting methodologies: the modern, fast-paced DevOps approach, and the standard, sedate, security implementation more suited to legacy software development. With microservices running in containers, communicating via APIs and deployed via automated CI/CD pipelines, traditional approaches to security must not only adapt to limit bottlenecks but be effective in the modern world.

Open source web application firewalls like ModSecurity and cloud-native security tools are regularly considered for additional protection in such cases, but are often found not to be as fast or comprehensive enough.

With organizations spending heavily on modern applications and infrastructure to stay competitive, anything that slows down that speed is seen as damaging to their investment. Like buying a sports car and using it to tow a trailer, security at the cost of performance is counterproductive and unpalatable to many.

To deliver both protection and speed, DevOps and SecOps must effectively join forces to become what's known as **"DevSecOps"**, a form of **"shift left"** for security that introduces the security side earlier and embeds it deeper within processes and tools. However, while that's good in theory, DevSecOps isn't so easy in practice. **Only 14% of organizations currently fully integrate security throughout the software development lifecycle.**[7]

So how can this friction between security and speed of deployment be overcome in an impactful and cost-effective manner? Automation is the answer.

A MODERN SOLUTION FOR MODERN APPLICATIONS

NGINX App Protect
Web Application Firewall

NGINX App Protect WAF is an application security solution that combines the efficiency of F5 Advanced Web Application Firewall (Advanced WAF) technology with the agility and performance of NGINX. Like the **“build once, run anywhere”** convenience of modern applications, automation in NGINX App Protect WAF delivers **“build once, adhere everywhere”** for security policies. A lightweight, modern solution, it reduces clashes between teams, saves time and money, and provides peace of mind that security best practices are being followed everywhere. It helps businesses to ensure both DevOps and SecOps can operate effectively and in harmony, so you can bring applications to market at speed without compromising security.

NGINX App Protect WAF supports multiple environments:

Cloud	Containers	CPUs	Operating Systems
• Amazon Web Services (AWS)	• Docker	• ARM (64 bit)	• CentOS
• Google Cloud Platform (GCP)	• Kubernetes	• PowerPC (64 bit)	• Debian
• Microsoft Azure	• OpenShift	• x86 (64 bit)	• Ubuntu
• VMware			

App-centric Security

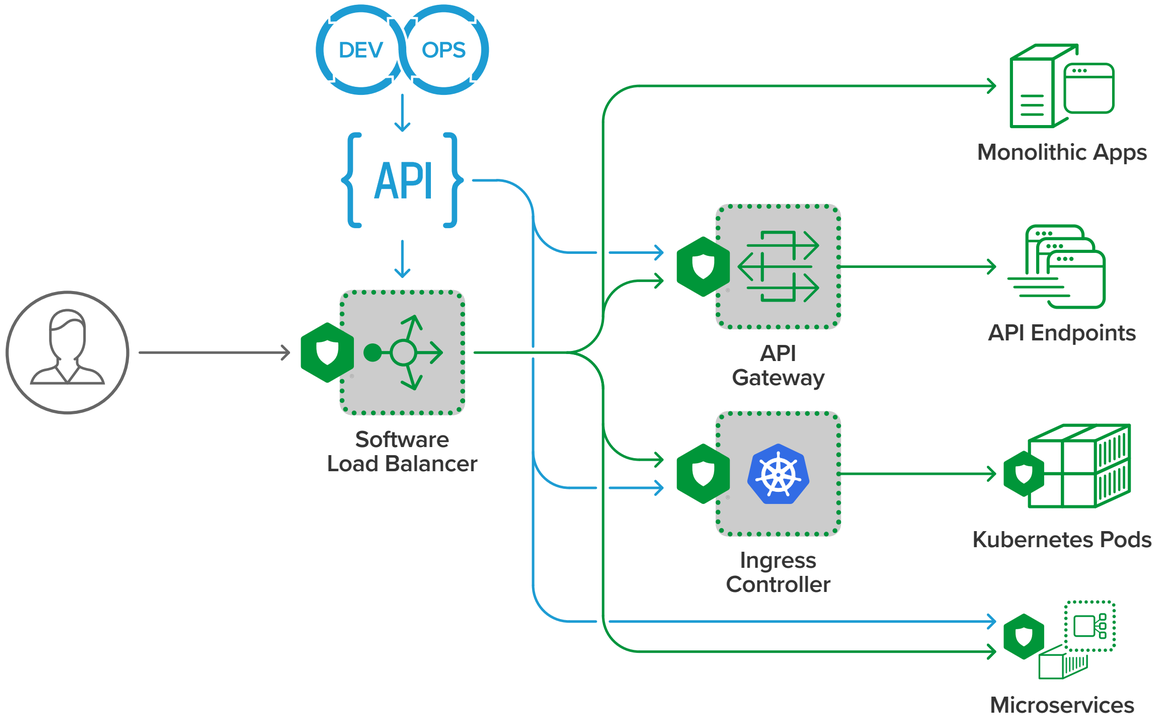
NGINX App Protect WAF’s security controls are ported directly from F5’s Advanced WAF technology, which puts it a cut above community-supported solutions like ModSecurity.

Its comprehensive set of WAF attack signatures has been extensively field-tested and proven, and its new violation model generates virtually no false positives. NGINX App Protect WAF protects against the OWASP Top 10 web application security risks, enforces protocol compliance, defends against common evasion techniques, provides denylisting, checks cookies, protects APIs, and prevents sensitive data leakage with F5’s Data Guard.

A MODERN SOLUTION FOR MODERN APPLICATIONS

Built for Modern Applications

There's no point deploying strong security if it can't be implemented in an application's operating environment. That's why NGINX App Protect WAF is designed to support modern application deployment topologies, such as the common deployment modes for F5 NGINX Plus. This includes Load Balancer, API Gateway, Ingress Controller for Kubernetes, Per-Service Proxy and Per-Pod Proxy. It's security that's designed for the modern world and the tools required to thrive within it.



Speed and Security Working as One

With NGINX App Protect WAF, you can make security bottlenecks a thing of the past without sacrificing performance for security or vice versa. ModSecurity, for example, conducts evaluation of regular expressions. That means that each additional control you add directly degrades application performance. As a result, many administrators choose to implement a very small number of controls to maintain speed at the expense of security. But NGINX App Protect WAF controls are compiled into bytecode, so traffic is processed at lightning-fast speeds regardless of how many attack signatures you enforce. The net result is up to 20x the throughput and requests per second compared to a ModSecurity implementation with the Core Rule Set v3 enabled.

App-Centric Security

Deploy trusted F5 controls close to your apps, protecting against revenue-impacting attacks, data theft, reputational damage, and regulatory non-compliance.

Built for Modern Apps

Deliver high-performance, scalable security on NGINX ADCs to enable consistent security controls for web applications, microservices, containers, and APIs.

CI/CD Friendly

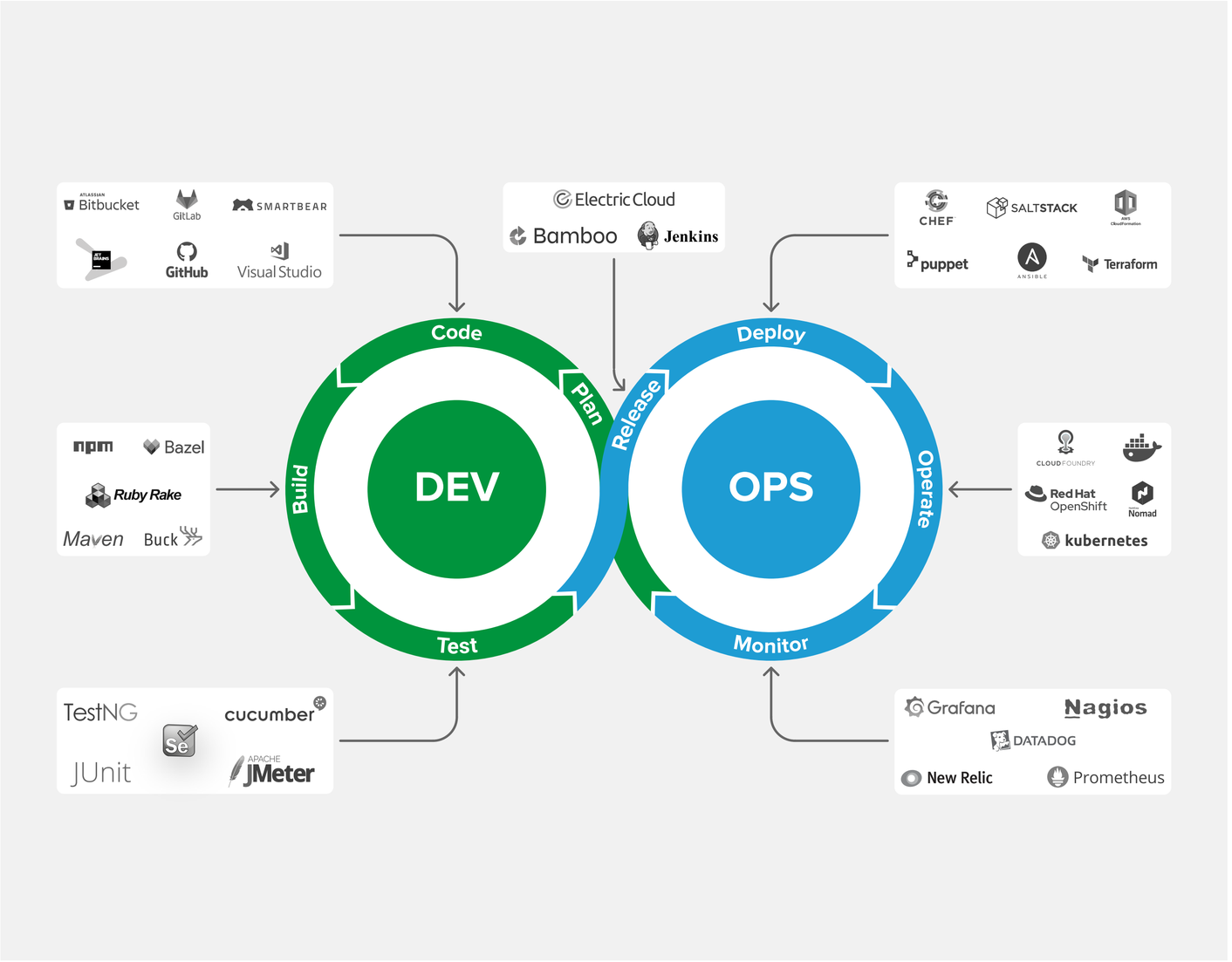
Centrally manage and automate approved security controls to remove workflow bottlenecks and support "shift left" Dev initiatives.

THE HARMONIZING EFFECT OF NGINX APP PROTECT WAF

As covered earlier in this eBook, many organizations wish to incorporate security practices into development sooner. But that's easier said than done. **While 65% of security teams report that they see a "shift left", less than a fifth are able to show proof of it.**[8] Worse still, **nearly half of enterprises admit to knowingly pushing vulnerable code to production due to time pressures.**[9]

Such security compromises often come down to the sluggish and disruptive nature of traditional security processes. Static application security testing (SAST) and software composition analysis (SCA), for example, can be effective at detecting security defects early in development. But what happens when vulnerabilities aren't spotted until after the application is released? Sending an app back to development not only increases costs and damages productivity, but also creates friction between DevOps and SecOps teams. The result: **48% of technical professionals believe security is a major constraint on their ability to deliver software quickly**.[10]

NGINX App Protect WAF helps to overcome these conflicts. It integrates into common development pipelines to remove friction and speed up secure deployment, with declarative configuration capabilities that mean security can become part of DevOps CI/CD automation and be tested just like any other part of an application's functional specification. In essence, the security policy and configuration are consumed as "code" pulled from a source code repository. The SecOps team creates and maintains security policy to ensure the controls required to protect the business are in place.



ENHANCED SECURITY AND COMPLIANCE

Powerful Perimeter Security

Before the introduction of a Zero Trust model, security was a simple matter of placing a perimeter around the intranet to separate it from the extranet, with the intranet presumed safe. Hackers quickly found ways around this, and that led to the advent of continual assessment where no entity is trusted by default.

Today's app architectures introduce their own security challenges as a result of being distributed across different locations, such as the cloud or on-premises servers, meaning they're no longer under the control of a local administrator. To protect modern apps, NGINX App Protect WAF acts as a gatekeeper, providing continual assessment on a perimeter around individual apps or groups of apps to inspect incoming traffic and enforce security policies. This can be applied to apps deployed on-premises, in the cloud or within a hybrid cloud, as well as for containerized architectures such as the Kubernetes framework.

Kubernetes Clusters Covered

NGINX App Protect WAF works with F5 NGINX Ingress Controller as the gatekeeper for an entire Kubernetes cluster, managing access from external clients and routing requests to the Kubernetes services in the cluster. But it also supports enforcing security policies at a more granular level within the cluster, either per-Pod or per-Service. With per-Pod protection, the Pod defines the perimeter containing an app or app component in one or more containers. With per-Service protection, a Service exposes the instances of an app deployment through one or more Pods. The perimeter is established around the Pods behind the Service.

With NGINX App Protect WAF, traffic inspection and access control eliminate threats before they cross the perimeter. As the last hop before the apps, it's the place where you can really see the type and number of threats against your apps.

ENHANCED SECURITY AND COMPLIANCE

Say "Yes" to PCI-DSS

To comply with the Payment Card Industry Data Security Standard (PCI DSS) and protect your apps against the ever-growing set of vulnerabilities, you need a modern WAF solution like NGINX App Protect WAF. The very first requirement of the PCI DSS11 for protecting cardholder data is to **"Install and maintain a firewall configuration to protect cardholder data."** It also states that owners of public-facing web applications must protect them by "installing an automated technical solution that detects and prevents web-based attacks: for example, a web application firewall." This isn't as simple as it sounds. With so many possible attacks and attack methods constantly changing, maintaining PCI DSS compliance is one of the most difficult challenges faced by modern applications.

Additional Protection

Beyond the 6,000 signatures NGINX App Protect WAF covers, it also performs HTTP protocol and evasion technique checks on a per-request basis to detect errors such as illegitimate metacharacters in the contents of the HTTP message, invalid length, and more. Such anomalies can indicate a potential zero-day exploit, and should raise concerns about other evidence that may exist in the traffic. It processes JSON and XML content, can check the payload for potentially malicious injections, and prevents responses from exposing sensitive information by masking the data (response scrubbing).

NGINX App Protect WAF in Action: reifen.com

A leading multi-channel provider of tires, wheels and tire-fitting services, **reifen.com** faced a very specific challenge: the German certification body TÜV required it to install a WAF in order to obtain the highest compliance rating as a trustworthy and secure online retailer. Because TÜV certifications are important to consumers, this became an essential priority.

For a number of years, reifen.com had already been using NGINX web servers to facilitate high-performance content delivery and initially considered NGINX Plus with Modsecurity, a solution that would have met the TÜV compliance requirements. However, after discussions with the F5 and NGINX teams, they ultimately chose NGINX App Protect WAF instead. The decision was influenced by NGINX App Protect WAF's superior performance levels, and its ability to futureproof against attack vectors that are likely to become more prevalent, such as attacks on their APIs.

"We decided to go with NGINX App Protect WAF because it gave us the best performance, the best long-term solution and the combined expertise of NGINX and F5 together," said Sascha Petranka, E-commerce Consultant to reifen.com. "Even though the cost was a little higher than ModSecurity, it was an obvious recommendation to make." As well as ensuring reifen.com could meet its new compliance requirements and earn the TÜV certification, NGINX Plus with NGINX App Protect WAF has helped the business gain visibility into its performance, identify problems more quickly, and respond to competitors with greater agility.

NGINX App Protect WAF is designed for modern infrastructures and can be installed anywhere, so it integrates directly into your CI/CD pipeline "as code". By being closer to your applications than traditional WAFs, it enables you to rapidly update security policies. Because NGINX App Protect WAF deploys on all platforms (public and private clouds, VMs, containers, and more) and use cases (including API Gateway, Ingress Controller for Kubernetes, and Lightweight Footprint in the Cloud), you get consistent performance and the same level of protection across your entire infrastructure. Furthermore, NGINX App Protect WAF covers more than 6,000 signatures, which are updated at least every two months to cover the latest known attacks. In short, NGINX App Protect WAF meets and exceeds PCI DSS requirements.

BOOST PERFORMANCE AND PEACE OF MIND WITH NGINX APP PROTECT WAF

NGINX App Protect
Web Application Firewall

NGINX App Protect WAF helps companies that have invested heavily in new application architectures and agile practices to enhance their ROI while ensuring their applications are secure and perform at their best. By fitting into development pipelines, it doesn't conflict with the processes of DevOps teams. NGINX App Protect WAF works in harmony with them, enabling you to deploy applications at speed while keeping them optimally protected. It streamlines application security and compliance, with high performance and extremely low false positives to give you peace of mind in an ever-more competitive online business world.

Seamless Integration with NGINX, the #1 Web Application Platform

- Enables strong security controls seamlessly integrated with NGINX Plus
- Outperforms other WAFs for improved user experience
- Reduces complexity and tool sprawl while delivering modern apps

Rapid Threat Defence and Security Analytics at Scale

- Provides expanded security beyond basic signatures to ensure adequate controls
- Utilizes F5 app security technology for efficacy superior to ModSecurity and others
- Builds on proven F5 expertise, so you can confidently run "blocking" mode in production
- Offers high-confidence signatures for extremely low false positives
- Increases visibility, integrating with third-party analytics solutions

Application Security as Agile as Your DevOps Processes

- Integrates security and WAF natively into the CI/CD pipeline
- Deploys as a lightweight software package that is platform agnostic
- Facilitates declarative policies for "security as code" and integration with DevOps tools
- Decreases developer burden and provides feedback loop for quick security remediation
- Accelerates time to market and reduces costs with DevSecOps-automated security

Discover how NGINX App Protect WAF can deliver 'build once, adhere everywhere' simplicity for your security policies and help bring your apps to market faster.

References

[1] https://www.thinkwithgoogle.com/marketing-strategies/app-and-mobile/mobile-page-speed-new-industry-benchmarks

[2] https://www.thinkwithgoogle.com/consumer-insights/consumer-trends/future-of-marketing-mobile-micro-moments

[3] https://www.nginx.com/wp-content/uploads/2020/05/2020-05-21-NGINX-App-Protect.pdf

[4] https://www.allthingsdistributed.com/2014/11/apollo-amazon-deployment-engine.html

[5] https://techjury.net/blog/how-many-cyber-attacks-per-day

[6] https://enterprise.verizon.com/resources/reports/dbir

[7] https://www.whitesourcesoftware.com/forrester-state-of-application-security-report

[8] https://about.gitlab.com/developer-survey

[9] https://www.prnewswire.com/news-releases/devsecops-study-finds-that-nearly-half-of-organizations-consciously-deploy-vulnerable-applications-due-to-time-pressures-301107632.html

[10] https://snyk.io/wp-content/uploads/dso_2020.pdf

[11] https://www.pcisecuritystandards.org/document_library

Test drive NGINX App Protect WAF with a 30-day free trial.
Register here: **nginx.com/free-trial-request**

About NGINX App Protect WAF

NGINX App Protect WAF is a modern application security solution that combines trusted F5 Advanced WAF technology with the agility and performance of NGINX Plus. As a lightweight, platform-agnostic, self-managed software module, NGINX App Protect WAF seamlessly integrates into your CI/CD pipeline as security as code for declarative security policies. This allows your business to build more reliable, secure, and risk-adverse applications. NGINX App Protect WAF enables DevOps and SecOps teams to work together in migrating towards a shift left strategy, so that enterprise organizations can bring applications to market at speed without compromising on security.

 **nginx.com**

 **nginx.com/contact-sales**

 **+1-888-882-7535**

©2022 F5, Inc. All rights reserved. NGINX, NGINX Ingress Controller, NGINX Plus, NGINX Unit, NGINX App Protect WAF, F5, the NGINX logo, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries.
Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5.