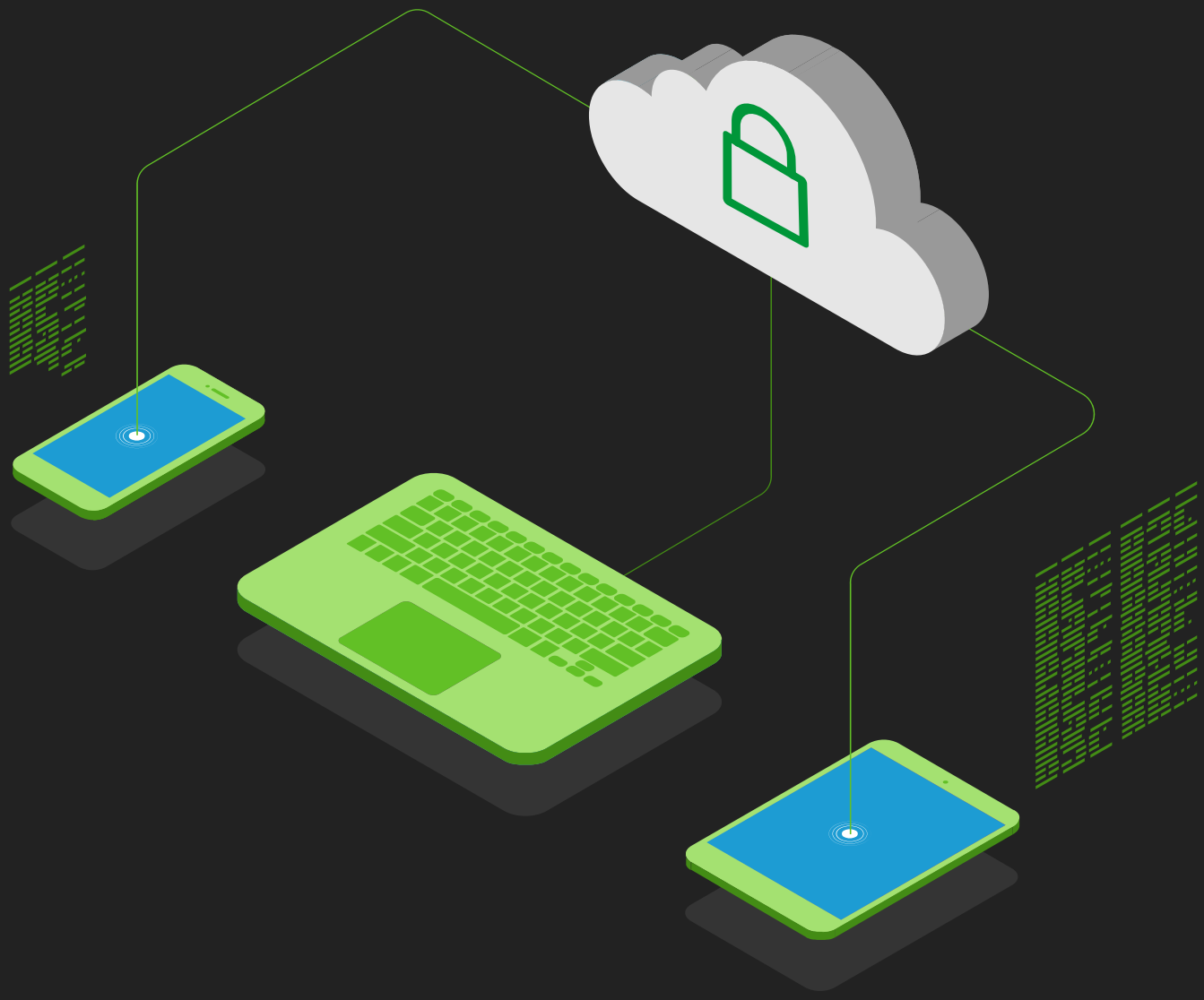
NGINX App Protect®
Web Application Firewall

Speed vs. Security

Protecting Modern Apps and APIs at the Pace of Modern Business



NGINX is a part of F5

Introduction

The pace of today's business world is driving a wedge between the way applications are developed and how they are protected. By harnessing the latest developments in infrastructure and applications, companies can better compete and adapt faster. However, they could also be jeopardizing security. This whitepaper looks at the changing nature of business applications and the ways in which traditional security approaches must change in order to keep up.

Today, 98% of organizations depend on applications to run or support their business.[1]

From Monolithic Apps to Microservices

To understand today's challenge and the security threats, it is important to appreciate how and why business applications have changed. It's a fact of the modern world that 98% of all businesses depend on applications to run or support their business operations.[1] Of those apps, the number built with microservices is growing apace, up from 40% in 2019 to 60% in 2020, with 54% of businesses using microservices in some or all of their apps.[2] The expectation is that by 2022, 90% of all new apps will feature microservices architectures.[3] These trends highlight not only why a business needs to keep on top of the latest developments in applications, but also the value of speed and agility when it comes to application deployment.

You're probably moving the same way, migrating from the monolithic apps of the old days to cloud-native technologies while also implementing DevOps principles. And with good reason.

No matter the sector, the business world has never been kind to those stuck in the past. Customers, partners and employees don't just demand the most from your technology-driven services; they expect it. Markets don't wait for companies to adapt; they simply move on without them.

This is why businesses simply have to ensure that their applications offer the best possible experience. And they can only deliver that experience by taking an active approach to application development: a faster, more iterative approach that provides the flexibility businesses need to remain competitive.

DevOps, microservices, and containers can all help to deliver this much sought-after application agility, overhauling old-fashioned approaches in favor of the delivery methods that today's customers expect. But what about other key considerations, like protecting those apps? Can security policies keep up with the pace?

What is an adaptive application?

The concept of an adaptive application is one that is more proactive and smarter than its traditional, monolithic counterparts. It harnesses modern technology to respond to its environment, automating redundant processes for greater efficiencies, scaling based on performance requirements and protecting itself. By combining all these attributes, adaptive applications can eliminate menial, repetitive tasks, provide peace of mind that they can take care of themselves, and enable developers to focus on what matters – delivering outstanding digital experiences.

A New Front-Line in the Battle Against Hacks

Hackers launch an average of 2,244 attacks per day. That's one every 39 seconds.[4] And a single successful attack is all it takes to wreak financial and reputational havoc on a business or even destroy it entirely. It might sound dramatic, but these are the odds your business faces today. That said, despite the average cost of a data breach in 2020 coming in at a hefty $3.86 million per company,[5] it's just 5% of the apps in an organization's portfolio, on average, that are properly protected.[6]

Even more worrying is how sophisticated and wide-ranging the attacks have become. Hackers no longer only target code. With 40% of attacks on web applications coming through APIs, and that number expected to grow to 90% in 2021,[7] higher walls simply don't provide the protection a modern environment needs. This increased threat level combined with today's ever-faster and more frequent release cycles, which give security flaws more of a chance to slip through the net, quickly adds up to a recipe for disaster.

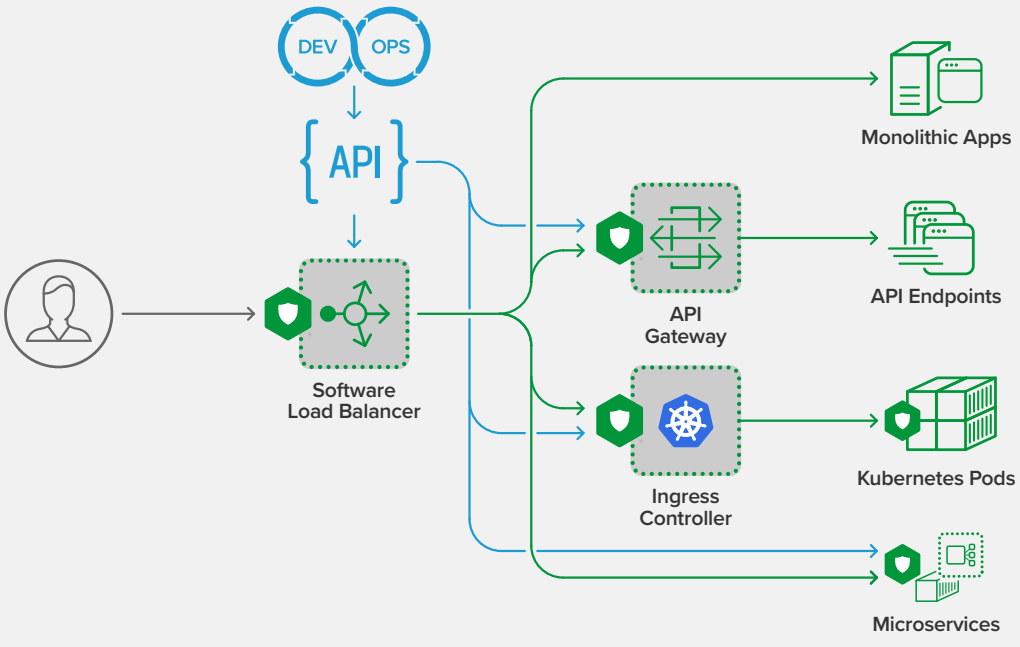
40% of attacks on web applications come through APIs and that number is expected to grow to 90% in 2021.[7]

Balancing Security Needs with Delivery Speed

No organization wants to restrict agility or limit innovation. Likewise, a company never wants to put its data nor that of its customers at risk. However, as the demands of the business world increase and modern application development has to move with the times to maintain a competitive edge, businesses are being forced to choose between the two. Either you go to market fast and leave yourself potentially exposed, or you operate slowly and securely but risk missing the boat. Does it really have to be this way?

Security policies were once applied during the final stages of a release, but the speed of deployments today makes that almost impossible. Given that there are an estimated 500 software developers for every security professional,[8] the odds are not stacked in favor of app protection.

In the end, the whole process hampers the ability to provide robust, consistent security across application architectures and infrastructure, and ensures that the blame never falls at any particular door. Business leaders understand the importance of security along with the need to get their apps to market fast. DevOps teams resent SecOps for slowing down deployment, and SecOps laments the lack of security controls DevOps provides. In fact, it turns out that 48% of technical professionals see security as the major roadblock to delivering software quickly.[9]



NGINX App Protect integrates with NGINX Plus running as a Software Load Balancer, API Gateway, Kubernetes Ingress Controller, Per-Service Proxy, or Per-Pod Proxy.

Searching for Security Simplicity

It's clear that for businesses to drive innovation and remain agile, the effectiveness of DevOps automation and its "build once, run anywhere" simplicity is crucial. But what if a "build once, adhere anywhere" approach could be applied to security policies? For an agile and secure way forward, businesses must find a way to integrate security into the lifecycle of an application, not apply it at the end of development or attempt to fix it with add-ons. Security and app development shouldn't simply co-exist: They have to become one.

Security and app development shouldn't simply co-exist: They have to become one.

The Best of Both Worlds

So, is there a way to achieve the utopia of DevSecOps? What would it mean for protection and release velocity if you could implement SecOps application security policies into DevOps without friction?

The first change this requires is one of mindset. Old-fashioned thinking has no place in today's application development environment, and all parties should embrace the idea of securing apps rather than seeing it as a hurdle to overcome. All teams should be pulling in the same direction, working toward the common goal of safe, high-quality applications delivered at speed. Integrated security needs to become a standard part of the development process, and the speed required to make that possible can be delivered in a number of ways, key among them being policy automation. What's also required is a lightweight security solution that overcomes the limitations of "checkbox" web application firewalls. It has to address the real security challenges facing modern DevOps environments by delivering high-performance, scalable security with consistent controls for web applications, microservices, containers, and APIs. It should trigger fewer false positives and, critically, it needs to be faster than other solutions. Such a solution should be CI/CD-friendly, centrally managing and automating approved security controls to remove workflow bottlenecks and support "shift left" DevOps initiatives. It needs to be supported by an experienced team and improve visibility while optimizing performance.

If you can have all that, the friction between DevOps and SecOps will disappear, and the conflict between rapid deployment and security will be a thing of the past. With the right tools and a more collaborative development culture delivering powerful, consistent protection that matches the pace of today's app development, businesses can achieve true peace of mind and deliver amazing experiences at speed.

NGINX App Protect
Web Application Firewall

Prevent Hacks and Bottlenecks with F5 NGINX App Protect WAF

If your organization is facing the challenges covered in this whitepaper, NGINX App Protect WAF could play a key part in improving the security of your applications and bringing DevOps and SecOps teams closer together. NGINX App Protect WAF is a lightweight security solution that enables businesses to bring applications to market at speed without compromising security. Providing app-centric security, it enables businesses to deploy trusted F5 controls close to their apps, protecting against revenue-impacting attacks, data theft, reputational damage, and regulatory non-compliance. Built on F5's many years of perfecting its market-leading WAF and bot protection, NGINX App Protect WAF streamlines application security and compliance. NGINX App Protect WAF's high performance, optimal protection, and extremely low false positives give you peace of mind in an increasingly competitive online business world.

References

[1] https://www.f5.com/state-of-application-services-report

[2] https://www.nginx.com/resources/datasheets/state-of-modern-app-delivery-2020-nginx-open-source-community

[3] https://www.nginx.com/resources/library/idc-report-apis-success-failure-digital-business

[4] https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

[5] https://www.ibm.com/security/data-breach

[6] https://www.varonis.com/2019-data-risk-report

[7] https://www.csoonline.com/article/3452747/what-you-need-to-know-about-the-new-owasp-api-security-top-10-list.html

[8] https://portswigger.net/daily-swig/githubs-nico-waisman-security-is-not-just-an-opportunity-but-a-responsibility-for-us

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

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

nginx.com

nginx.com/contact-sales

+1-888-882-7535

NGINX
Part of F5