NGINX App Protect®

Speed Vs. Security – Protecting modern apps and APIs at the pace of modern business

NGINX is a part of F5

Introduction

The pace of modern business is driving a wedge between the way applications are developed and how they are protected. By harnessing modern infrastructure and applications, companies can better compete and adapt faster, but could also be jeopardising 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.

From monolithic apps to microservices

To understand the challenge and the security threats posed, it is important to appreciate how and why business applications have changed. Today, 98% of organisations depend on applications to run or support their business[1]. Of those apps, the number built with microservices is growing at pace, up from 40% in 2019 to 60% in 2020, with 54% of businesses using microservices in some or all of their apps[2]. By 2022, it's expected that 90% of all new apps will feature microservices architecture[3]. These trends not only highlight the importance of modern applications to businesses, but the value of achieving speed and agility when it comes to their deployment.

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

Across sectors, modern business isn't kind to those stuck in the past. Customers, partners and employees don't just demand more from your technology-driven services; they expect it. Markets don't wait for companies to adapt; they simply forget about them.

This is why businesses are being forced to take action, ensuring their applications offer the best possible experience. But delivering these experiences requires a different 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 favour of modern delivery methods. But what about other key considerations like protecting those apps? Can security policies handle the pace?

A new front line in the battle against breaches

Hackers launch an average of 2,244 attacks per day. That's one every 39 seconds[4]. And a single successful malicious act is all that's required to wreak financial and reputational havoc on a business or even destroy it entirely. It might sound drastic, but these are the odds organisations face today. However, despite the average cost of a data breach in 2020 weighing in at $3.86 million per company[5], on average only 5% of the apps in an organisation's portfolio are properly protected[6].

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

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.

Even more worrying is how much more sophisticated and wide-ranging the attacks are. 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 required protection in modern environments. Couple this increased threat level with faster and more frequent release cycles where security flaws can easily slip through the net, and it can quickly become a recipe for disaster.

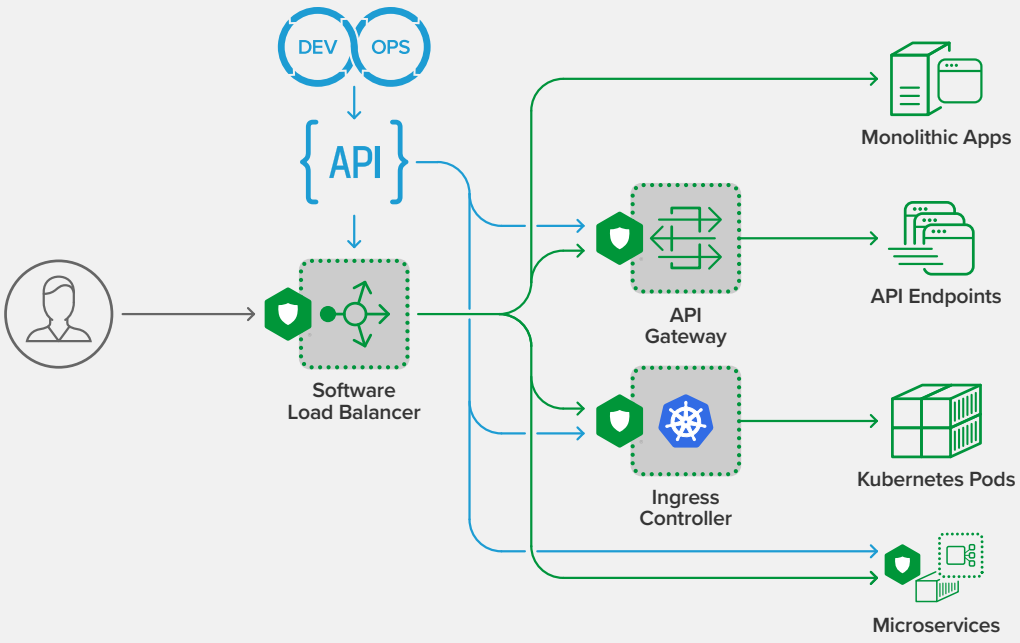
With 40% of attacks on web applications coming through APIs and that number expected to grow to 90% in 2021[7]

Balancing security needs with delivery speed

No organisation wants to restrict agility or limit innovation. Likewise, companies aren't willing to put their data or that of their customers at risk. However, as the demands of modern business increase and modern application development is required to maintain a competitive edge, businesses are being forced to choose between the two. Either you go to market fast and potentially exposed, or you operate slowly and securely. It shouldn't be this way.

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

And so, the ability to provide robust, consistent security across application architectures and infrastructure is hampered, with blame falling at no particular door. Business leaders understand the importance of security but also the need to get their apps to market fast. DevOps teams resent the slowing of deployment by SecOps and SecOps laments the lack of security controls DevOps provides. In fact, 48% of technical professionals see security as the major blocker to delivering software quickly[9].



NGINX App Protect integrates with NGINX Plus running as a software load balancer, API gateway, Kubernetes Ingress Controller, and sidecar 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. So, 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 mustn't simply co-exist but become one.

Security and app development mustn't simply co-exist but become one.

The best of both worlds

So, is there a way to achieve the eutopia 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 required is mindset. Old fashioned thinking has no place in a modern application development environment, and all parties should embrace the idea of securing apps, not see it as a hurdle to be 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 for it to do so 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 must 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, crucially, it must 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" Dev initiatives. It should be supported by an experienced organisation and improve visibility while optimising performance.

If the above can be achieved, the friction between DevOps and SecOps is removed, and the fight between rapid deployment and security becomes a forgotten issue. With the right tools and a more collaborative development culture delivering powerful, consistent protection that matches the pace of modern app development, businesses can achieve true peace of mind and deliver amazing experiences at speed.

NGINX App Protect

Prevent breaches and bottlenecks with NGINX App Protect

If your organisation is facing the challenges covered in this whitepaper, NGINX App Protect could play a key part in improving the security of your applications and bringing DevOps and SecOps teams closer together. NGINX App Protect is a lightweight, modern 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 Advanced WAF technology perfected by F5 over many years, NGINX App Protect streamlines application security and compliance. With high performance, optimal protection and extremely low false positives it provides peace of mind in an ever more 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

Partner overview

LumIT develops IT solutions to meet its customers' real needs with an innovative approach. Since 2009, this Italian System Integrator has been studying and implementing both established and cutting-edge Cyber Security technologies and today is among the first in Italy to offer IT Automation services.

lumit.it

info@lumit.it

+39 02 36589110

NGINX Part of F5