NGINX App Protect®

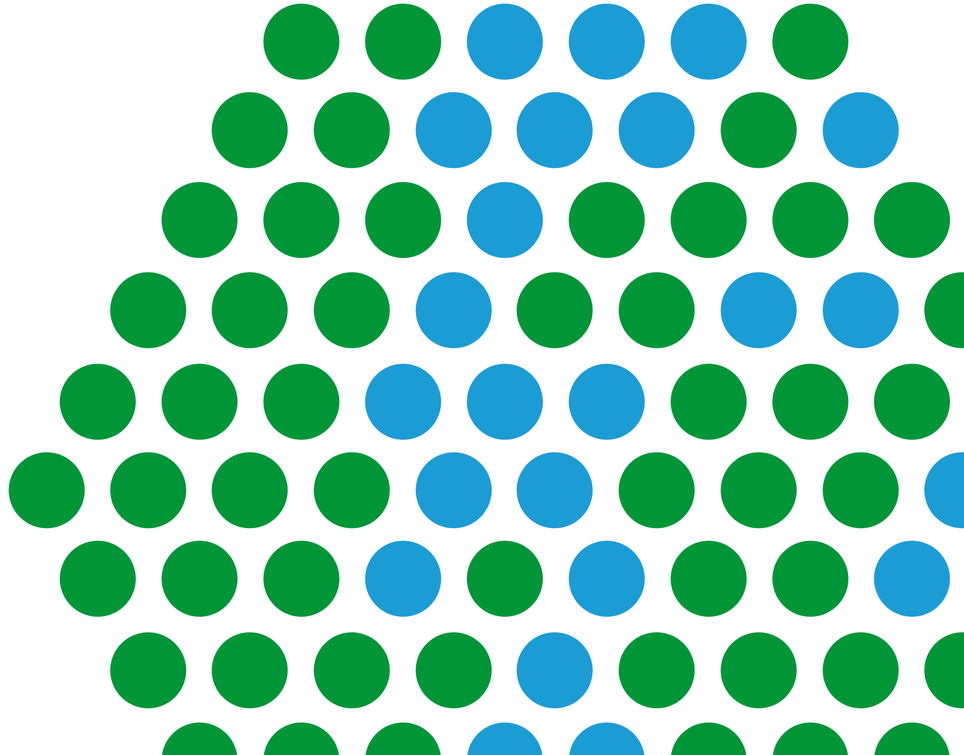
THE SECRET TO MODERN APPLICATION SECURITY

How NGINX App Protect can help your organisation prevent downtime and breaches by securing your modern apps and APIs

NGINX is a part of F5

CONTENTS

NGINX App Protect.



THE IMPORTANCE OF PACE IN MODERN APPLICATION DEVELOPMENT

Every business wants to be agile. They want to adapt quickly to the latest trends, keep up with competitors and better serve their customers and employees. In essence, they need to move faster than ever before.

In today's business world, the way to do that is through modern applications and APIs, and a lot of companies are already making use of them.

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

They use microservices architecture to operate at the pace of modern business and harness DevOps to rapidly design, deploy and redefine applications as required. The speed of this agile software development, featuring continuous integration and deployment comes from a far heavier reliance on automation. Adaptive applications of this nature are built to be redefined quickly and frequently to deliver business innovation at a pace to match 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 and increasing loyalty.

With the business market ever more competitive, 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. It's why modern application development methods are so popular, but they also have a negative side effect when it comes to security.

Performance matters

Google research has found that customer expectations are rising dramatically and that they 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 liklihood[1].

Elsewhere,

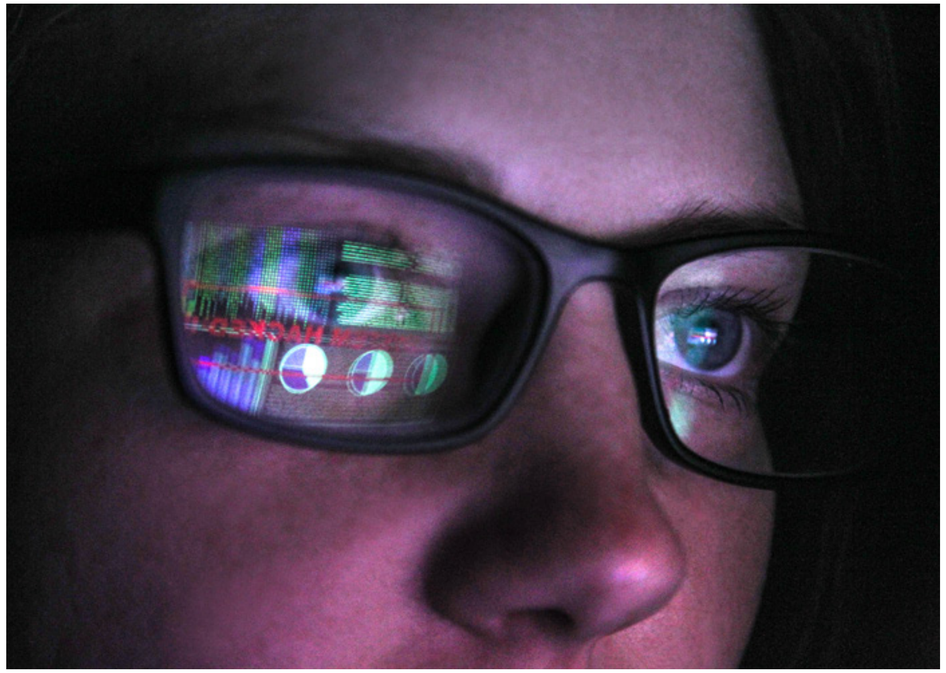
53%

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

This is crucial information for businesses, with the performance of their applications directly impacting customer experience and sales.

SECURITY SLOWDOWNS INTRODUCE FRICTION

Traditional application development saw security teams apply their policies and carry out checks at the end of the process. However, today, the pace of deployment makes it impossible for them to cope. If you take an extreme example from back in 2015, **Amazon hit 50 million production deployments in a year[4].** Roughly one deployment per second. How can traditional protection methods possibly hope to match this frantic pace? This leaves businesses with a tough decision to make. Do they slow down development in the modern environments they've invested heavily in to ensure adequate protection for their apps, or do they continue at speed with inadequate security controls? 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.

Over 30,000 websites are hacked per day, with an attack 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]**. However, any weak point within an entire application stack is now a potential risk, with the decentralised nature of modern applications providing a far larger attack surface. 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 where a castle and moat approach was effective for keeping the bad guys out of an internal network, modern applications are the new front line. The point where the network meets a user. Any user. And those users may not always have positive intentions.

TRADITION VS. TRANSFORMATION

The root of the problem is conflicting methodologies. The modern, fast-paced DevOps approach and 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 adapt to not only limit bottlenecks but be effective in the modern world.

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

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

To deliver both protection and pace, DevOps and SecOps must effectively join forces to become what's known as 'DevSecOps', part of a "shift left" for security whereby it is introduced earlier and is more embedded within processes and tools. However, while sound in theory, DevSecOps isn't so easy in practice, with only 14% of organisations fully integrating 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? The answer lies in automation.

A MODERN SOLUTION FOR MODERN APPLICATIONS

NGINX App Protect

NGINX App Protect 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 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 practice is being followed everywhere. It helps businesses to ensure both DevOPs and SecOps can operate effectively and in harmony, with applications brought to market at speed without compromising security.

NGINX APP Protect supports multiple environments

Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure
- VMware

Containers
- Docker
- Kubernetes
- OpenShift

CPUs
- ARM (64 bit)
- PowerPC (64 bit)
- x86 (64 bit)

Operating Systems
- CentOS
- Debian
- Ubuntu

App-centric security

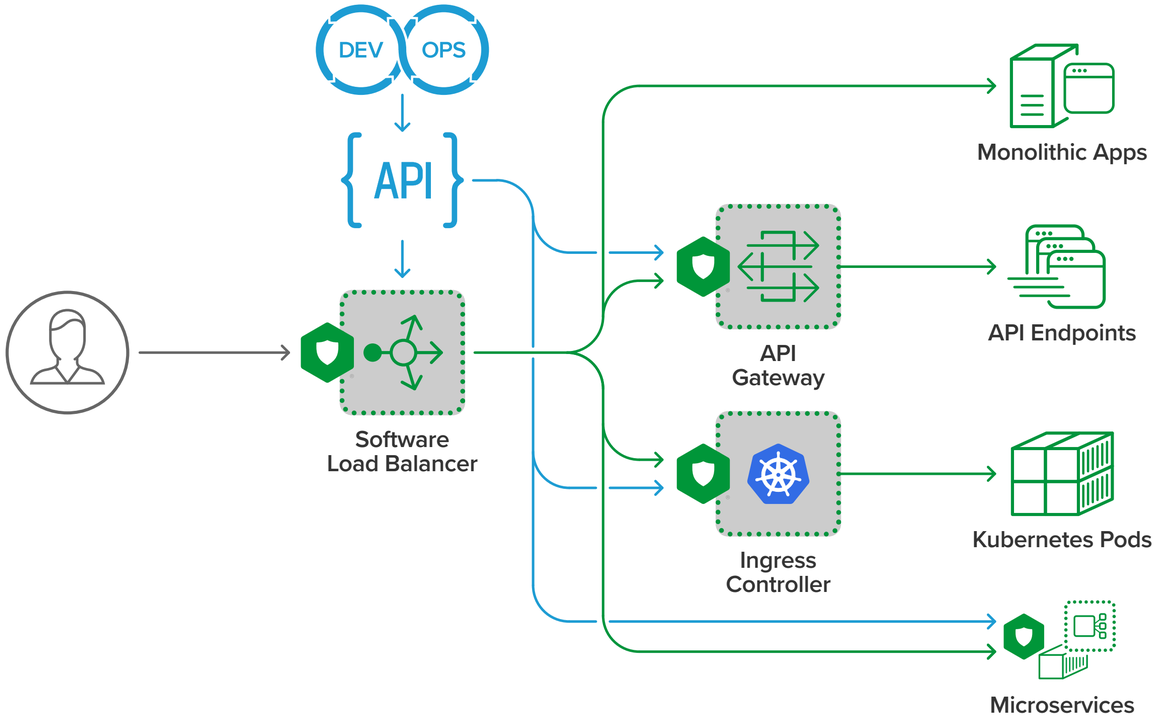
NGINX App Protect's security controls are ported directly from F5's Advanced WAF technology, which makes it a cut above community supported solutions like ModSecurity.

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 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 controls if they can't be implemented in an application's operating environment. That's why NGINX App Protect is designed to support modern application deployment topologies, such as the common deployment modes for NGINX Plus. This includes Load balancer, API gateway, Ingress controller for Kubernetes Pods and Per-Pod proxy for microservices. 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, the security slowdowns of the past can be eliminated, with no need to sacrifice performance for security, and vice versa. If you take ModSecurity, for example, it involves 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. However, NGINX App Protect 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 Rules 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

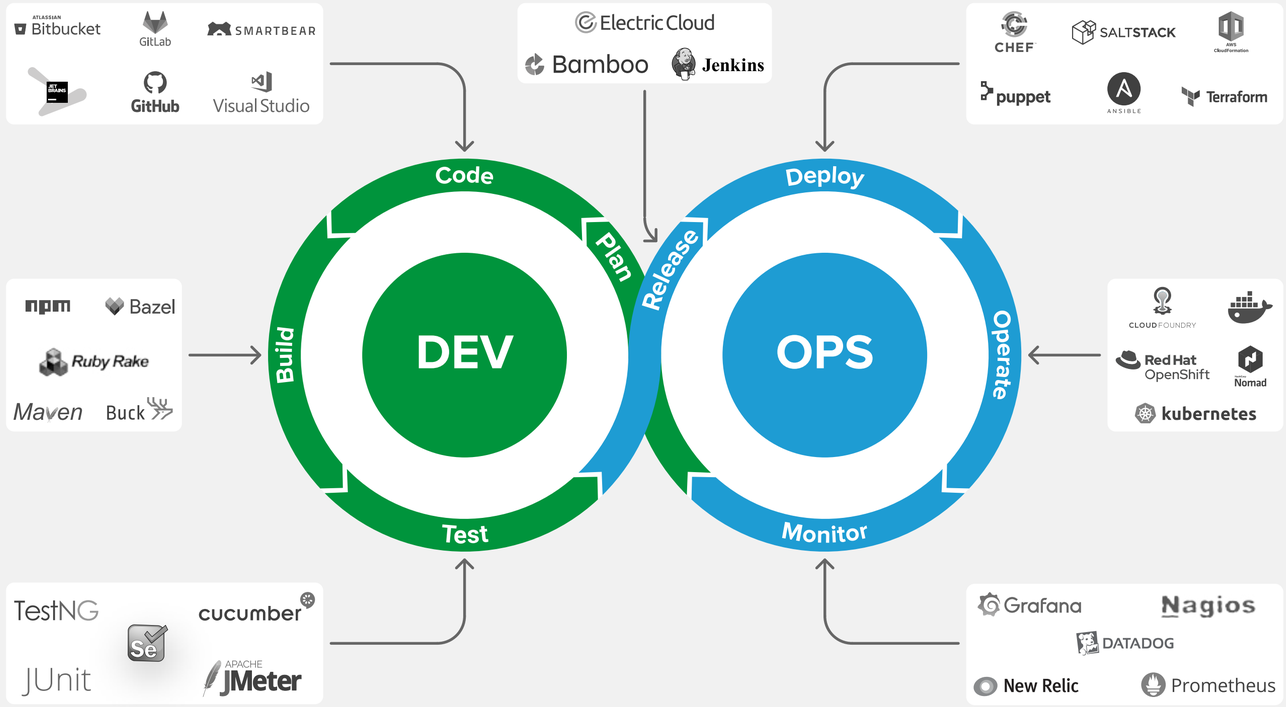
CI/CD Friendly

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

THE HARMONISING EFFECT OF NGINX APP PROTECT

As covered earlier in this eBook, many organisations wish to incorporate security practices earlier into development. However, it's easier said than done. **While 65% of security teams report 'shifting 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 are often 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? Not only does sending an app back to development increase cost and damage productivity, it also creates friction between DevOps and SecOps teams, with **48% of technical professionals believing security is a major constraint on their ability to deliver software quickly[10].** NGINX App Protect helps to overcome such 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

Security, before the introduction of a Zero Trust model, 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, leading to the advent of continual assessment where no entity is trusted by default.

New 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 becomes 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 containerised architectures such as the Kubernetes framework.

Kubernetes clusters covered

NGINX App Protect works with NGINX Plus 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. However, security policies can be enforced at a more granular level within the cluster as well, 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, traffic inspection and access control eliminate threats before they cross the perimeter. As the last hop before the apps, it is where you can best 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. The very first requirement of the PCI DSS[11] to protect 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 a number of attacks possible and attack methods constantly changing, maintaining PCI DSS compliance is one of the most significant challenges faced by modern applications.

Supplementary protection

Beyond the 6,000 signatures NGINX App Protect 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 possible attack that is unknown (zero day) and their presence reinforces other evidence that may exist in the traffic. It processes JSON and XML content and can check the payload for potentially malicious injections and prevents responses from exposing sensitive information by masking the data (AKA response scrubbing).

App Protect in action: reifen.com

A leading multi-channel provider of tires, wheels and tire-fitting services, **reifen.com** faced a very specific challenge. 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, it became an essential priority.

reifen.com had already been using NGINX web servers for a number of years 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, it opted instead for NGINX App Protect. The decision was influenced by App Protect's superior performance levels, and its ability to future-proof against attack vectors that are likely to become more prevalent, such as attacks on their APIs.

"We decided to go with App Protect 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 App Protect has helped the business gain visibility into its performance, identify problems more quickly and respond to competitors with greater agility.

Because NGINX App Protect is designed for modern infrastructure and can be installed anywhere, it slots 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 deploys on all platforms (public and private clouds, VMs, containers, and more) and use cases (including API gateway and Kubernetes Ingress controller), you get consistent performance and the same level of protection across your entire infrastructure. Furthermore, NGINX App Protect covers more than 6,000 signatures that are updated at least every two months to cover the latest known attacks. In short, NGINX App Protect meets and exceeds PCI DSS requirements.

BOOST PEACE OF MIND AND PERFORMANCE WITH NGINX APP PROTECT

NGINX App Protect

NGINX App Protect 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 but works in harmony with them, enabling applications to be deployed at speed and optimally protected. It streamlines application security and compliance and with high performance and extremely low false positives, it provides 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
- Utilises F5 app-security technology for efficacy superior to ModSecurity and others
- Builds on proven F5 expertise, so you can confidently run in "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 agnostic of underlying infrastructure
- 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 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/doibrary

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