NGINX App Protect®

NGINX
Part of F5

Moderne Anwendungssicherheit

Ausfallzeiten und Sicherheitsverletzungen verhindern – durch den Schutz Ihrer modernen Apps und APIs

Die Anwendungslandschaft hat sich dramatisch verändert.

Fast 85 % der neuen Workloads werden in Containern bereitgestellt und 83 % des Internetverkehrs sind mittlerweile API-Calls.

Und die Risiken steigen.

30.000 Websites werden pro Tag gehackt und 64 % der Unternehmen weltweit waren bereits Ziel mindestens einer Form von Cyberangriffen[1].

Und dennoch spielt das Thema Sicherheit in der modernen Anwendungsentwicklung oft zu spät eine Rolle.

Im Durchschnitt verursacht eine Datenschutzverletzung Kosten in Höhe von 3,92 Millionen US-Dollar. Trotzdem sind nur 5 % der Apps im Portfolio eines Unternehmens ordnungsgemäß geschützt[1]. Grund dafür sind häufig gegensätzliche Überlegungen von DevOps und SecOps.

Um eine schnelle Bereitstellung sowie eine optimale Sicherheit und Compliance für verteilte moderne App-Umgebungen zu erreichen, müssen DevOps-Teams:

- vom Sicherheitsteam autorisierte unterbrechungsfreie Sicherheitskontrollen in ihre Automatisierungs- und CI/CD-Prozesse integrieren.
- App-Sicherheitskontrollen in verteilten Umgebungen wie Containern und Microservices bereitstellen und managen.
- kostengünstige Sicherheitskontrollen implementieren, ohne dadurch die Release-Geschwindigkeit oder die Anwendungsleistung zu beeinträchtigen.

NGINX App Protect

NGINX App Protect stellt eine effektive und harmonische Arbeit von sowohl DevOps als auch SecOps sicher. Auf diese Weise können Unternehmen Anwendungen schnell auf den Markt bringen – ohne Kompromisse bei der Sicherheit. Basierend auf der bzw. dem marktführenden WAF und Bot-Schutz, die von F5 über viele Jahre perfektioniert wurden, optimiert NGINX App Protect die Anwendungssicherheit und Compliance. Mit hoher Leistung, optimalem Schutz und einer extrem niedrigen Fehlalarmquote erhalten Sie Sicherheit in einer immer wettbewerbsintensiveren Online-Geschäftswelt.

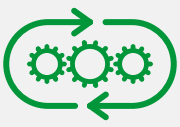
Warum NGINX App Protect?

App-zentrierte Sicherheit

Die Implementierung vertrauenswürdiger Kontrollen von F5 in der Nähe Ihrer Apps schützt vor umsatzschädigenden Angriffen, Datendiebstahl, Rufschädigung und Rechtsverstößen.

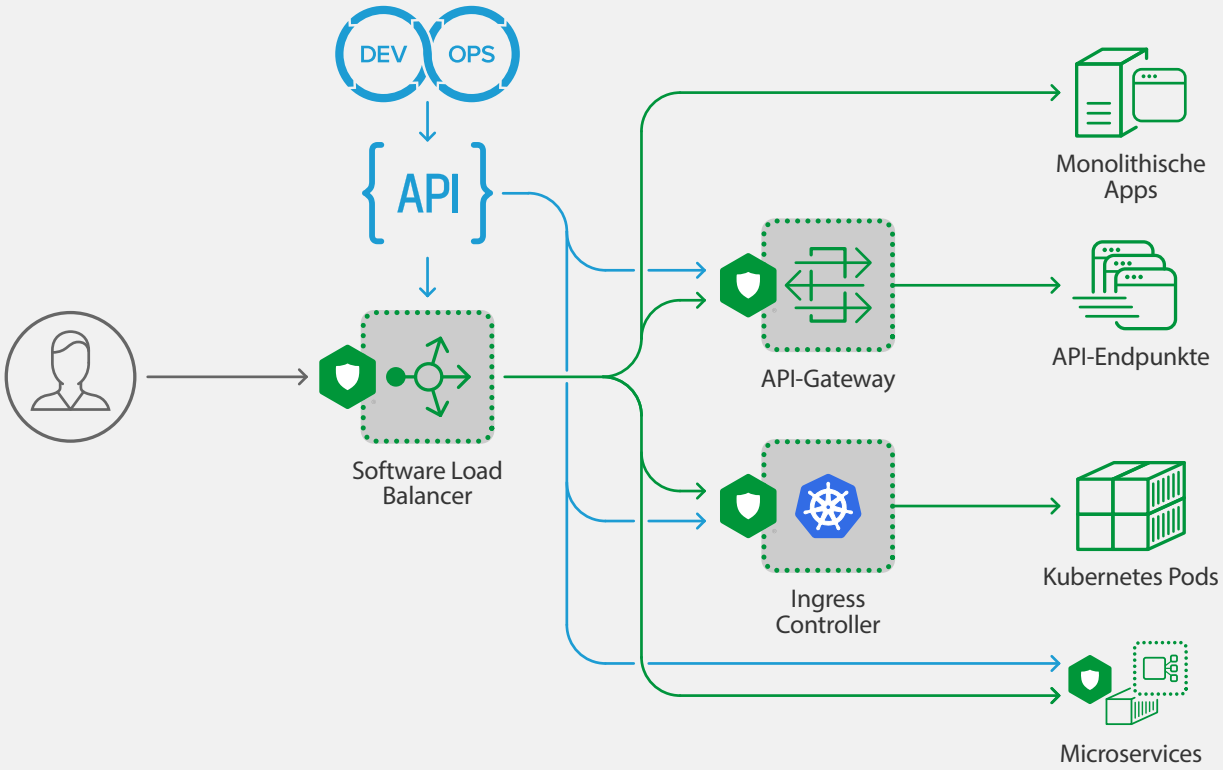
Entwickelt für moderne Apps

Die leistungsstarke, skalierbare Sicherheit auf den ADCs von NGINX ermöglicht konsistente Sicherheitskontrollen für Webanwendungen, Microservices, Container und APIs.



CI/CD-freundlich

Das zentrale Management und die Automatisierung genehmigter Sicherheitskontrollen beseitigen Engpässe im Workflow und unterstützen „Shift left“ bei DevOps-Initiativen.



NGINX App Protect lässt sich in NGINX Plus integrieren, das als Software Load Balancer, API-Gateway, Kubernetes Ingress Controller und Sidecar Proxy ausgeführt wird.

Funktionen von NGINX App Protect

Nahtlose Integration mit NGINX Plus

- Ermöglicht starke Sicherheitskontrollen, die nahtlos in NGINX Plus integriert sind.
- Übertrifft andere WAFs für eine verbesserte Benutzererfahrung.
- Reduziert Komplexität und die Zahl der benötigten Tools und unterstützt gleichzeitig moderne Apps.

Schnelle Abwehr von Bedrohungen und umfassende Sicherheitsanalysen

- Bietet erweiterte Sicherheit über grundlegende Signaturen hinaus, um angemessene Kontrollen zu gewährleisten.
- Nutzt die App-Sicherheitstechnologie von F5, deren Effizienz ModSecurity und anderen überlegen ist.
- Baut auf bewährtem Know-how von F5 auf, sodass Sie während der Entwicklung sicher im „Blocking“-Modus arbeiten können.
- Bietet hochgradig zuverlässige Signaturen für eine extrem niedrige Anzahl von Fehlalarmen.
- Erhöht die Sichtbarkeit durch Integration mit Analyselösungen von Drittanbietern.

Anwendungssicherheit – genauso agil wie Ihre DevOps-Prozesse

- Integriert Sicherheit und WAF nativ in die CI/CD-Pipeline.
- Bereitgestellt als schlankes Softwarepaket, das unabhängig von der zugrundeliegenden Infrastruktur ist.
- Erleichtert deklarative Richtlinien für „Sicherheit als Code“ und die Integration mit DevOps-Tools.
- Verringert den Entwickleraufwand und schafft eine Feedbackschleife für eine schnelle Wiederherstellung der Sicherheit.
- Beschleunigt die Markteinführung und senkt die Kosten mit automatisierten DevSecOps.

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

Unterstützte Umgebungen

Cloud

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

Container

- Docker
- Kubernetes
- OpenShift

CPUs

- x86 (64 Bit)

Betriebssysteme

- CentOS
- Debian
- Red Hat Enterprise Linux
- Ubuntu

Informieren Sie sich, wie NGINX App Protect auch Sie unterstützen kann

techmatrix CONSULTING GMBH
www.techmatrix.de
sales@techmatrix.de
+49 89 121 914 55