NGINX App Protect®

Hız mı Güvenlik mi?
Modern uygulamalarınızı ve API'lerinizi, modern iş hızına göre koruyun!

NGINX is a part of F5

Giriş

Modern iş dünyasındaki hızlı değişim, uygulamaların geliştirilmesi ve korunmasında kullanılan yöntemlerin arasını açmakta. Şirketler, modern altyapı ve uygulamalardan yararlanarak daha iyi rekabet edebilir ve daha hızlı uyum sağlayabilir, ancak aynı zamanda güvenliği de tehlikeye atabilir. Bu kitapçıkta iş uygulamalarının değişen doğasını ve buna ayak uydurmak için geleneksel güvenlik yaklaşımlarının nasıl değişmesi gerektiği konusu mercek altına alınmıştır.

Bugün, kuruluşların %98'i işlerini devam ettirmek veya desteklemek için uygulamalara güveniyor(1)

Monolitik uygulamalardan mikro hizmetlere

Ortaya çıkan zorlukları ve güvenlik tehditlerini anlamak için, iş uygulamalarının nasıl ve neden değiştiğini anlamak önemlidir. Bugün, kuruluşların %98'i işlerini yürütmek veya desteklemek için uygulamalara güveniyor(1). Bu uygulamalardan, mikro hizmetler ile oluşturulan sayı, 2019'da %40 iken 2020'de %60'a çıkmıştır; işletmelerin %54'ü uygulamalarının bir kısmında veya tamamında mikro hizmetlerden yararlanmaktadır(2). 2022'ye kadar, tüm yeni uygulamaların %90'ının mikro hizmet mimarisine sahip olması beklenmektedir(3). Bu eğilimler, modern uygulamaların işletmeler için önemini vurgulamanın yanı sıra kullanımda elde dilen hız ve çevikliğe ulaşmanın değerini de ortaya koymaktadır.

Haklı olarak, eski monolitik uygulamalardan bulut tabanlı teknolojilere geçiş esnasında, aynı zamanda DevOps ilkelerini de uygularken, muhtemelen aynı şekilde hareket ediyorsunuzdur.

Modern iş dünyasında, sektörlerde geçmişte sıkışmış ve kendini güncelleyememiş olan şirketler ilerideki dönemlerde kaybetmeye mahkum olur. Müşteriler, iş ortakları ve çalışanlar yalnızca teknoloji odaklı hizmetlerinizden daha fazlasını talep etmiyor; bunu bekliyorlar.

Uyarlanabilir uygulama nedir?

Uyarlanabilir uygulamalar, geleneksel, monolitik muadillerinden daha proaktif ve daha akıllı uygulamalardır. Çevresine yanıt vermek, daha yüksek verimlilik için yedekleme süreçlerini otomatik hale getirmek, performans gereksinimlerine göre ölçeklendirmek ve kendisini korumak amacıyla modern teknolojiden yararlanır. Tüm bu özelliklerin bir arada kullanıldığı uyarlanabilir uygulamalar, sıradan, tekrar eden görevleri ortadan kaldırabilir, kendi başlarına hareket etme rahatlığı sunabilir ve bu sayede geliştiricilerin önemli olan noktalara odaklanmasını sağlayarak olağanüstü dijital deneyimler sunabilir.

Bu nedenledir ki; işletmeler, uygulamalarının mümkün olan en iyi seviyede deneyim sunmasını sağlamak için bir takım tedbirler almak zorunda kalmaktadır. Ancak bu deneyimleri sunmak, uygulama geliştirmeden farklı bir yaklaşım gerektirir. İşletmelerin rekabet güçlerini koruyabilmeleri için ihtiyaç duydukları esnekliği sunan daha hızlı, daha yenilikçi bir yaklaşım.

DevOps, mikro hizmetler ve konteynerlerin tümü, modern uygulama yöntemleri adına, eski moda yaklaşımları tamamen elden geçirerek, çokça aranan buteknolojik talebinkarşılanmasına yardımcı olabilmektedir. Peki, bu uygulamaların korunması gibi diğer önemli hususlar ne olacak? Güvenlik politikaları hız konusunun üstesinden gelebilir mi?

İhlallere karşı mücadelede yeni bir cephe

Bilgisayar korsanları günde ortalama 2.244 saldırı gerçekleştiriyor. Bu, her 39 saniyede bir saldırı anlamına geliyor(4). Ve başarıyla sonuçlanan bir tek saldırı, bir işletmeye mali ve itibar açısından zarar vermek ve hatta onu tamamen yok etmek için yeterli. Kulağa korkunç gelse de, bunlar bugün kuruluşların karşılaştığı tehlikeler. Bununla birlikte, 2020 yılında şirket başına 3,86 milyon ABD doları tutarında(5) ortalama veri ihlali maliyetine rağmen, bir kuruluşun portföyündeki uygulamaların ortalama olarak yalnızca %5'i uygun şekilde korunmaktadır(6).

Daha da endişe verici olan, saldırıların ne kadar karmaşık ve kapsamlı olduğudur. Bilgisayar korsanları artık yalnızca kodu hedeflemiyor. Web uygulamalarına yönelik saldırıların % 40'ının API'lar üzerinden geliyor olması ve bu sayının 2021 yılında %90'a çıkmasının bekleniyor olması(7), yüksek duvarların modern ortamlarda gerekli korumayı sağlamadığının bir göstergesidir. Bu artan tehdit düzeyi ile birlikte, güvenlik açıklarının ağ üzerinde kolayca oluşabileceği daha hızlı ve daha sık yayın döngüleri göz önünde bulundurulduğunda, bir felaketin yaşanmasının elbette kaçınılmaz olacağı aşikardır.

Web uygulamalarına yönelik saldırıların %40'ı API'ler üzerinden geliyor ve bu sayının 2021'de %90'a çıkması bekleniyor(7).

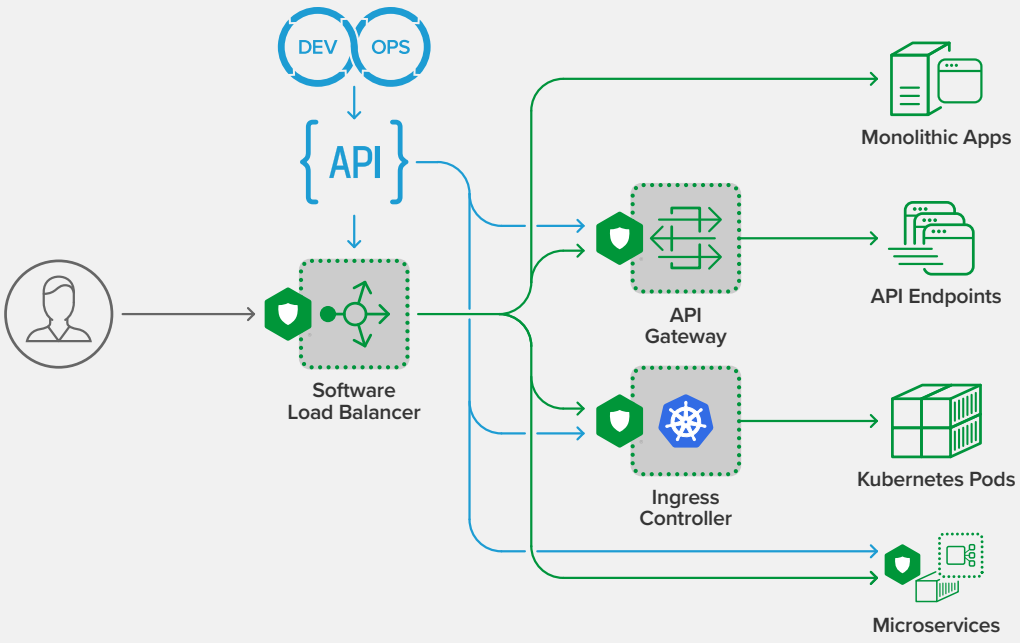
Uyulama hızıyla güvenlik ihtiyaçlarının dengelenmesi

Hiçbir kuruluş çevikliği kısıtlamayı veya inovasyonu sınırlamayı istemez. Aynı şekilde, şirketler de kendi verilerini veya müşterilerine ait verileri riske atmak istemez. Bununla birlikte, modern işletmelerin talepleri arttıkça ve rekabet gücünün korunması için modern uygulamalar geliştirmeye ihtiyaç duyuldukça, işletmeler ikisi arasında seçim yapmak zorunda kalmaktadır. Ya pazara hızlı girip tehditlere potansiyel olarak maruz kalırsınız ya da yavaş ve güvenli bir şekilde ilerlemeyi seçersiniz. Ancak, bu şekilde olmamalı.

Güvenlik politikaları, eskiden bir yayının son aşamalarında uygulanırken, bugün kullanım hızı bunu neredeyse imkansız hale getiriyor. Her güvenlik profesyoneli için tahmini 500 yazılım geliştiricisi olduğu düşünüldüğünde(8), ihtimaller elbette uygulamaların koruması yönünde olmayacaktır.

Ve bu nedenle, uygulama mimarileri ve altyapısı genelinde sağlam ve tutarlı güvenlik elde etme kabiliyeti, ihmal her hangi bir kimsenin üzerine atılmadan engellenmiş olur. İş dünyasının liderleri, güvenliğin öneminin yanı sıra uygulamaların hızlı bir şekilde pazara sunulması gerektiğinin de bilincinde.

DevOps ekipleri, SecOps tarafından kullanımın yavaşlatılmasına karşı çıkıyor ve SecOps da, DevOps'un sağladığı güvenlik kontrollerinin eksikliğinden yakınıyor. Aslında, teknik uzmanların %48'i güvenliği, yazılımı hızlı bir şekilde sunmanın önündeki en büyük engel olarak görmekte(9).



NGINX App Protect, yazılım yük dengeleyici, API ağ geçidi, Kubernetes Giriş Denetleyicisi ve yardımcı araç proxy'si olarak çalışan NGINX Plus ile entegre halde işlev görür.

Güvenlikte sadelik arayışı

İşletmelerin inovasyonu teşvik etmesi ve çevikliğini korumaları için, DevOps otomasyonunun etkinliği ve 'bir kez kur, her yerde kullan' basitliğinin son derece önemli olduğu açıktır. Öyleyse, 'bir kez kur, her yerde kullan' yaklaşımı güvenlik politikalarına uygulanabilse ne olur? Geleceğe yönelik, çevik ve güvenli bir yöntem için, işletmeler güvenliği uygulamanın ve yaşam döngüsüne entegre etmenin bir yolunu bulmalı, geliştirme işleminin sonunda uygulamamalı veya eklentilerle düzeltmeye çalışmamalıdır. Güvenlik ve uygulama geliştirme sadece bir arada yer almamalı, aynı zamanda tek vücut olarak ele alınmalıdır.

Güvenlik ve uygulama geliştirme sadece bir arada yer almamalı, aynı zamanda tek vücut olarak ele alınmalıdır.

Hem hızda hem güvenlikte en iyisi

Peki, DevSecOps'un ütopyasına ulaşmanın bir yolu var mı? Her hangi bir uyumsuzluk yaşamadan SecOps uygulama güvenliği politikalarını DevOps içerisinde uygulayabilseydiniz, bu koruma ve yayınlama hızı açısından ne anlama gelirdi?

Gerekli ilk değişiklik, zihniyettir. Eski moda düşüncenin, modern bir uygulama geliştirme ortamında yeri yoktur ve tüm taraflar, uygulamaları güvence altına alma fikrini benimsemeli, bunu aşılması gereken bir engel olarak görmemelidir. Tüm ekipler aynı yönde hareket etmeli ve hızlı bir şekilde sunulan güvenli, yüksek kaliteli uygulamaların hedeflendiği ortak amaç doğrultusunda çalışmalıdır. Entegre güvenlik, geliştirme sürecinin standart bir parçası haline gelmelidir ve bunu yapması için gereken hız, politika otomasyonu gibi yöntemler dahil olmak üzere pek çok farklı yolla sağlanabilir. Buna ilave olarak ihtiyaç duyulan, "checkbox" web uygulaması güvenlik duvarlarının sınırlamalarının üstesinden gelen hafif bir güvenlik çözümüdür. Web uygulamaları, mikro hizmetler, konteynerler ve API'lar için istikrarlı kontrollerle yüksek-performanslı, ölçeklenebilir güvenlik sunarak modern DevOps ortamlarının karşılaştığı gerçek güvenlik sorunlarını ele almalıdır. Daha az miktarda yanlış pozitif tetiklemeli ve en önemlisi diğer çözümlerden daha hızlı olmalıdır. Bu türden bir çözüm, CI/CD dostu olmalı, iş akışında yaşanan darboğazları ortadan kaldırmak için onaylı güvenlik denetimlerini tek noktadan olarak yönetmeli ve otomatikleştirmeli ve "shift left" Dev inisiyatiflerini desteklemelidir. Deneyimli bir kuruluş tarafından desteklenmeli ve performansı optimize ederken görünürlüğü arttırmalıdır.

Yukarıdakilerin gerçekleşmesi durumunda, DevOps ve SecOps arasındaki uyumsuzluk ortadan kalkar ve hızlı kullanım ile güvenlik arasındaki savaş geçmişte kalır. Doğru araçlar ve modern uygulama geliştirme hızına uygun güçlü ve tutarlı koruma sağlayan daha işbirlikçi bir geliştirme kültürü ile, işletmeler gerçek bir rahatlama yaşayabilir ve hızlı bir şekilde muhteşem uygulamalar gerçekleştirebilir.

NGINX App Protect

NGINX App Protect ile ihlalleri ve darboğazları önleyin!

Kuruluşunuz bu kitapçıkta ele alınan zorluklarla karşı karşıyaysa, NGINX App Protect, uygulamalarınızın güvenliğini artırma ve DevOps ile SecOps ekiplerini birbirine yakınlaştırmada önemli bir rol oynayabilir. NGINX App Protect, işletmelerin uygulamaları güvenlikten ödün vermeden hızla piyasaya sunmasını sağlayan hafif, modern bir güvenlik çözümüdür. Uygulama-merkezli güvenlik sağlayarak, işletmelerin uygulamalarına yakın olan güvenilir F5 kontrollerini kullanmalarına, gelirleri-etkileyen saldırılara, veri hırsızlığına, itibar kaybına ve yasalara uyum durumuna karşı koruma elde etmelerini sağlar. Uzun yıllar boyunca F5'in mükemmel hale getirdiği Gelişmiş WAF teknolojisi üzerine inşa edilen NGINX App Protect, uygulama güvenliğini ve uyum durumunu kolaylaştırır. Yüksek performans, optimal koruma, son derece düşük yanlış alarm oranı ile, işinizi huzurla devam ettirmenizi ve rekabetçi ortamda bir adım öne geçmenizi sağlar.

Referanslar

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/github-s-nico-waisman-security-is-not-just-an-opportunity-but-a-responsibility-for-us
9. https://snyk.io/wp-content/uploads/dso_2020.pdf

Exclusive Networks

Exclusive Networks olarak, firmaların dijital dönüşüm yolculuklarında, altyapı sistemlerinin güvenliğini ve sürekliliğini sağlamak en önemli görevimiz.
Benzersiz stratejilerimiz ile, iş ortaklarımıza daha çok fırsat sağlıyor ve müşteri ilişkilerini güçlendirmelerine yardımcı oluyoruz. Bizim uzmanlığımız, onların gücü – sürekli gelişen teknolojileri ve değişen iş modellerini yönetebilmeleri için, onlara uçtan uca eğitimler ve profesyonel hizmetlerimiz ile, destek veriyoruz.
Exclusive Networks'ün hikayesi, tüm Dünya'ya yayılmış, 'önce hizmet' anlayışı ile, yeniliği ve özgünlüğü birleştirmiş, sektörün büyüme hızının da önüne geçmiştir. 100 ülkede, 50'den fazla ofisimizle, eşsiz 'Global vizyon, yerel çözümler' modelini benimsiyoruz.

https://www.exclusive-networks.com/tr/

Eduyuru@exclusive-networks.com

+90 216 464 0490

© 2021 F5, Inc. Her hakkı saklıdır. NGINX, NGINX Controller, NGINX Plus, NGINX Unit, NGINX App Protect, F5, NGINX logosu ve F5 logosu, ABD'de ve diğer bazı ülkelerde F5'in ticari markalarıdır. Diğer F5 ticari markaları, f5.com'da tanımlanmıştır. Burada atıfta bulunulan diğer tüm ürünler, hizmetler veya şirket adları, F5'ile doğrudan veya dolaylı bir bağlantılı olmaksızın, ilgili sahiplerinin ticari markaları olabilir.

NGINX Part of F5