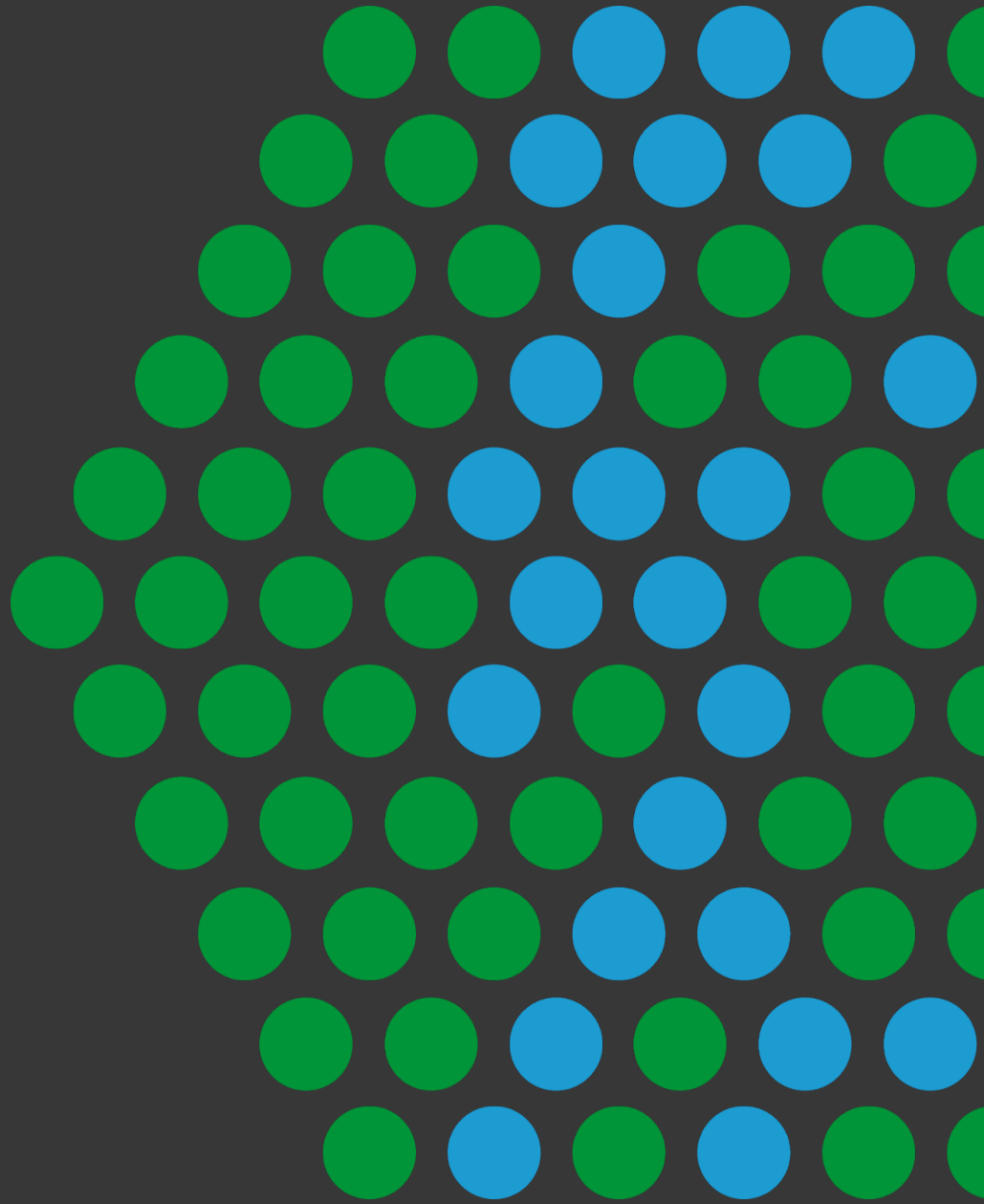
NGINX
Part of F5

Обзор NGINX

ЧТО ЕЩЕ ЕСТЬ У NGINX КРОМЕ NGINX

Александр Серебряков
Старший Инженер Решений, sasha@f5.com

2021

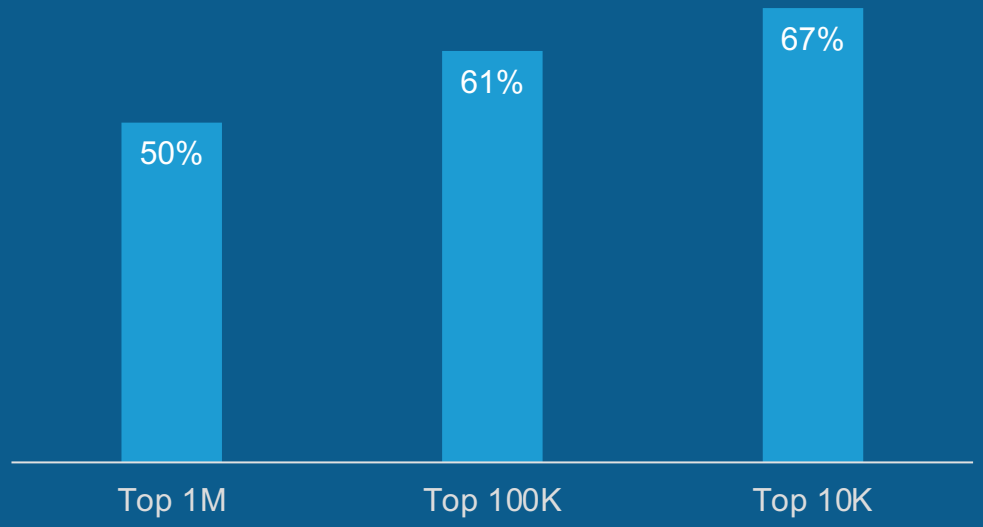


№1

“Большинство сайтов используют NGINX”

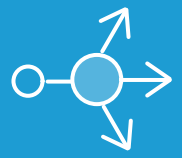
Источник: Netcraft April 2019 Web Server Survey

Самые загруженные ресурсы используют NGINX



Источник: W3Techs Web server ranking, 07-May-2019

Web Server
Reverse Proxy
and Cache

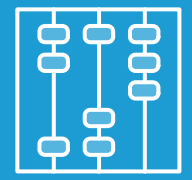


Advanced Load Balancing

Advanced Content Cache

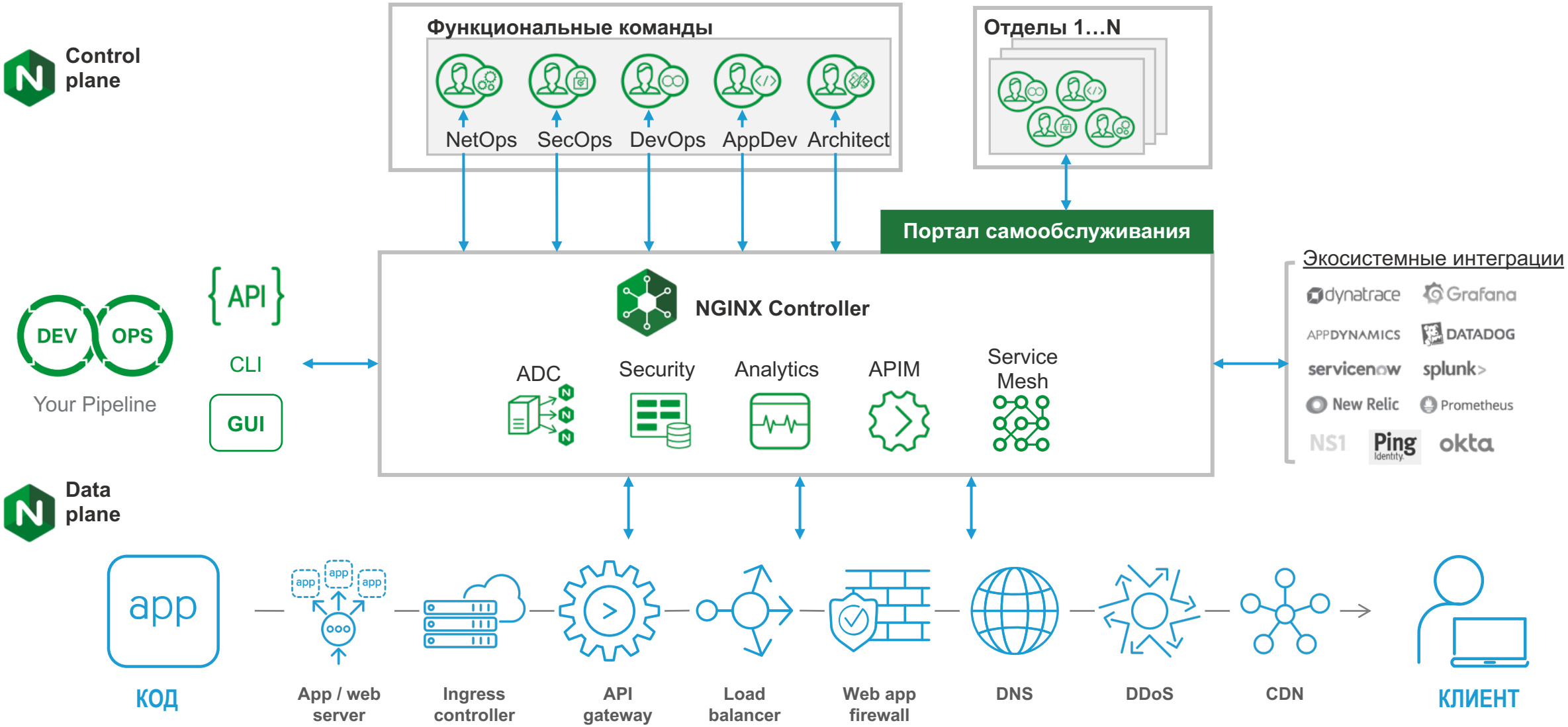
Web Server Reverse Proxy and Cache

Advanced Security Controls



Advanced Monitoring & Management

Что представляет из себя NGINX сегодня



Любая инфраструктура

Containers ● Public cloud ● Virtual machines ● Colocation ● Commodity HW ● Purpose-built HW

NGINX Part of F5

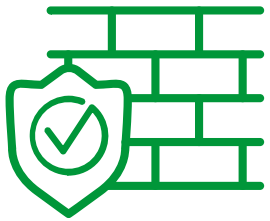
NGINX решения и наши темы сегодня

NGINX Plus

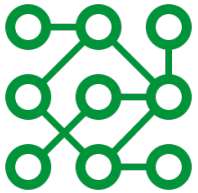
NGINX Controller

NGINX Instance Manager

API Management



NGINX App Protect



Ingress Controller and Service Mesh

NGINX Plus

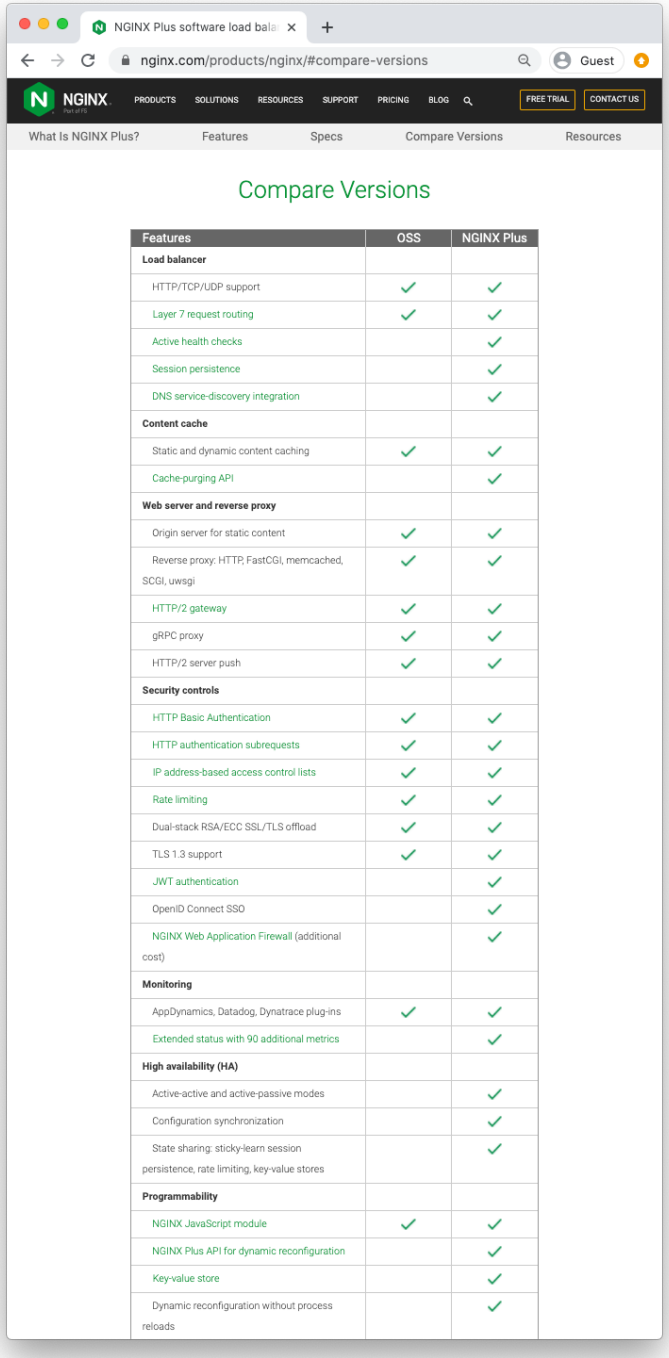
Примеры использования NGINX Plus

ГДЕ И КАК ОН МОЖЕТ БЫТЬ ПОЛЕЗЕН

Возможность NGINX Plus

КАКИЕ ФУНКЦИИ ЕСТЬ ТОЛЬКО В NGINX PLUS

1. **Балансировка нагрузки (алгоритмы на основе времени, sticky sessions, active health checks)**
2. **Мониторинг (API и >100 метрик, а также дашбоард)**
3. **Динамическая конфигурация (API, Service Discovery, key-value store)**
4. **Высокая доступность и кластер (keepalived, cluster sync)**
5. **Аутентификация (JWT, OpenID Connect)**
6. **Web Application Firewall**
7. **Валидированные сторонние модули**



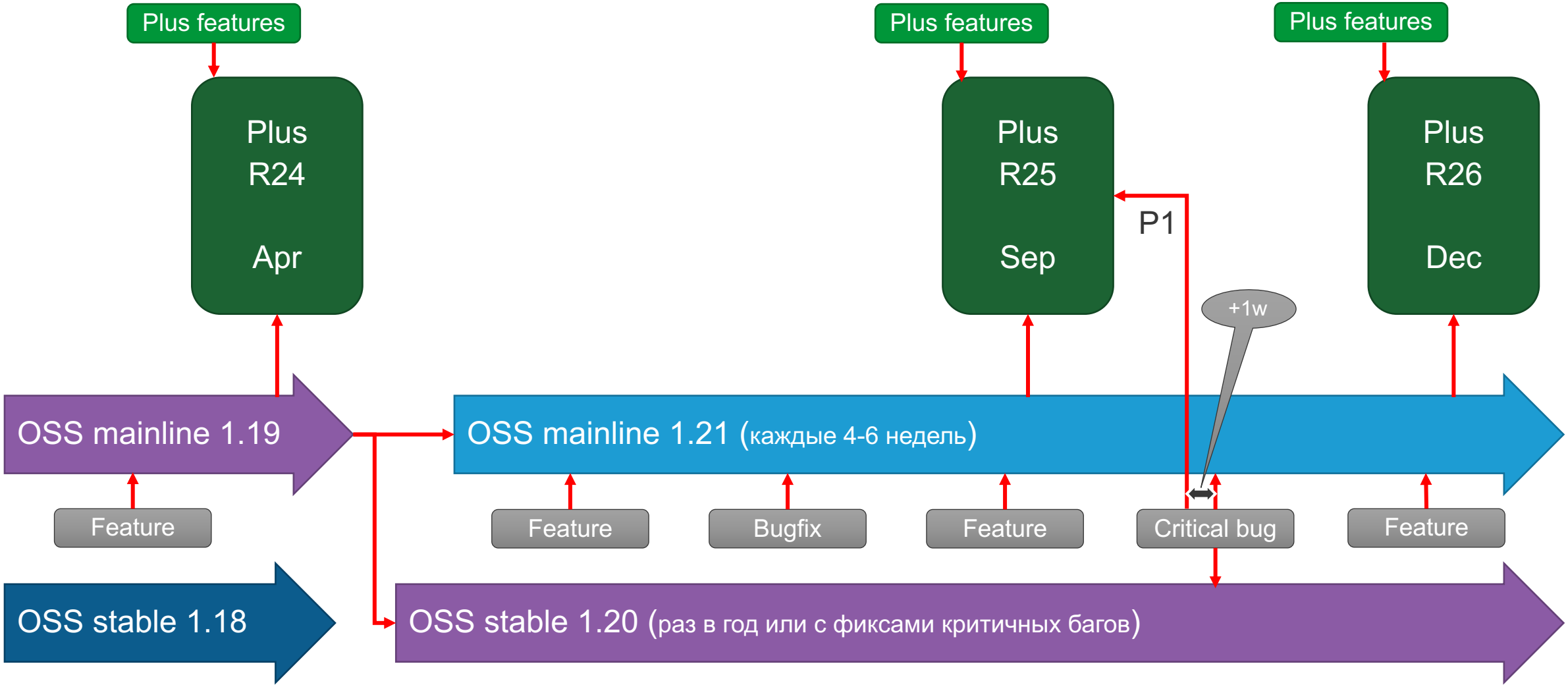
Features	OSS	NGINX Plus
Load balancer		
HTTP/TCP/UDP support	✓	✓
Layer 7 request routing	✓	✓
Active health checks		✓
Session persistence		✓
DNS service-discovery integration		✓
Content cache		
Static and dynamic content caching	✓	✓
Cache-purging API		✓
Web server and reverse proxy		
Origin server for static content	✓	✓
Reverse proxy: HTTP, FastCGI, memcached, SCGI, uwsgi	✓	✓
HTTP/2 gateway	✓	✓
gRPC proxy	✓	✓
HTTP/2 server push	✓	✓
Security controls		
HTTP Basic Authentication	✓	✓
HTTP authentication subrequests	✓	✓
IP address-based access control lists	✓	✓
Rate limiting	✓	✓
Dual-stack RSA/ECC SSL/TLS offload	✓	✓
TLS 1.3 support	✓	✓
JWT authentication		✓
OpenID Connect SSO		✓
NGINX Web Application Firewall (additional cost)		✓
Monitoring		
AppDynamics, Datadog, Dynatrace plug-ins	✓	✓
Extended status with 90 additional metrics		✓
High availability (HA)		
Active-active and active-passive modes		✓
Configuration synchronization		✓
State sharing: sticky-learn session persistence, rate limiting, key-value stores		✓
Programmability		
NGINX JavaScript module	✓	✓
NGINX Plus API for dynamic reconfiguration		✓
Key-value store		✓
Dynamic reconfiguration without process reloads		✓

Почему вам пригодится NGINX Plus

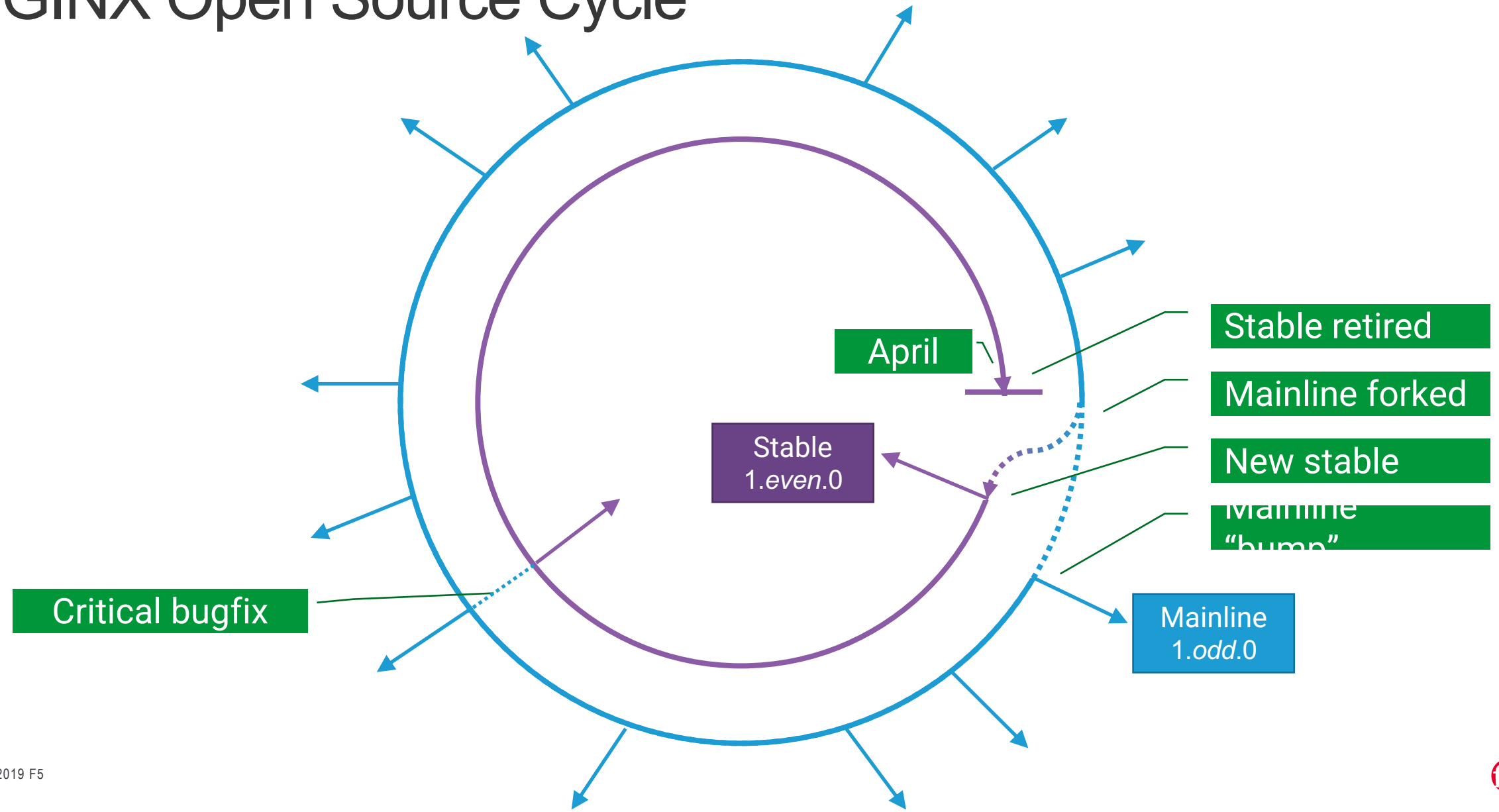
НЕ ТЕХНИЧЕСКИЕ ПРЕИМУЩЕСТВА СИСТЕМЫ

1. **Техническая поддержка** – одна из лучших в индустрии (Stevie Gold, 9.7/10)
2. **Дополнительные возможности** – функции доставки приложений Enterprise класса
3. **Плановые выпуски ПО** – устойчивая каденция (апрель, сентябрь, декабрь)
4. **Полностью протестированное ПО** – дополнительное тестирование NGINX
5. **Сертификация** –сертифицируем ОС с сертифицированными модулями (3rd party)
6. **Проактивные обновления безопасности** – Bug Fixes/Hot Fixes
7. **Помощь с документацией по продукту** – советы, уточнения, разработка
8. **Влияние на направление продукта** – предоставление планов, доступ к разрабам
9. **Конфиденциальность** – получить помощь в частном порядке, а не на общедоступном форуме поддержки

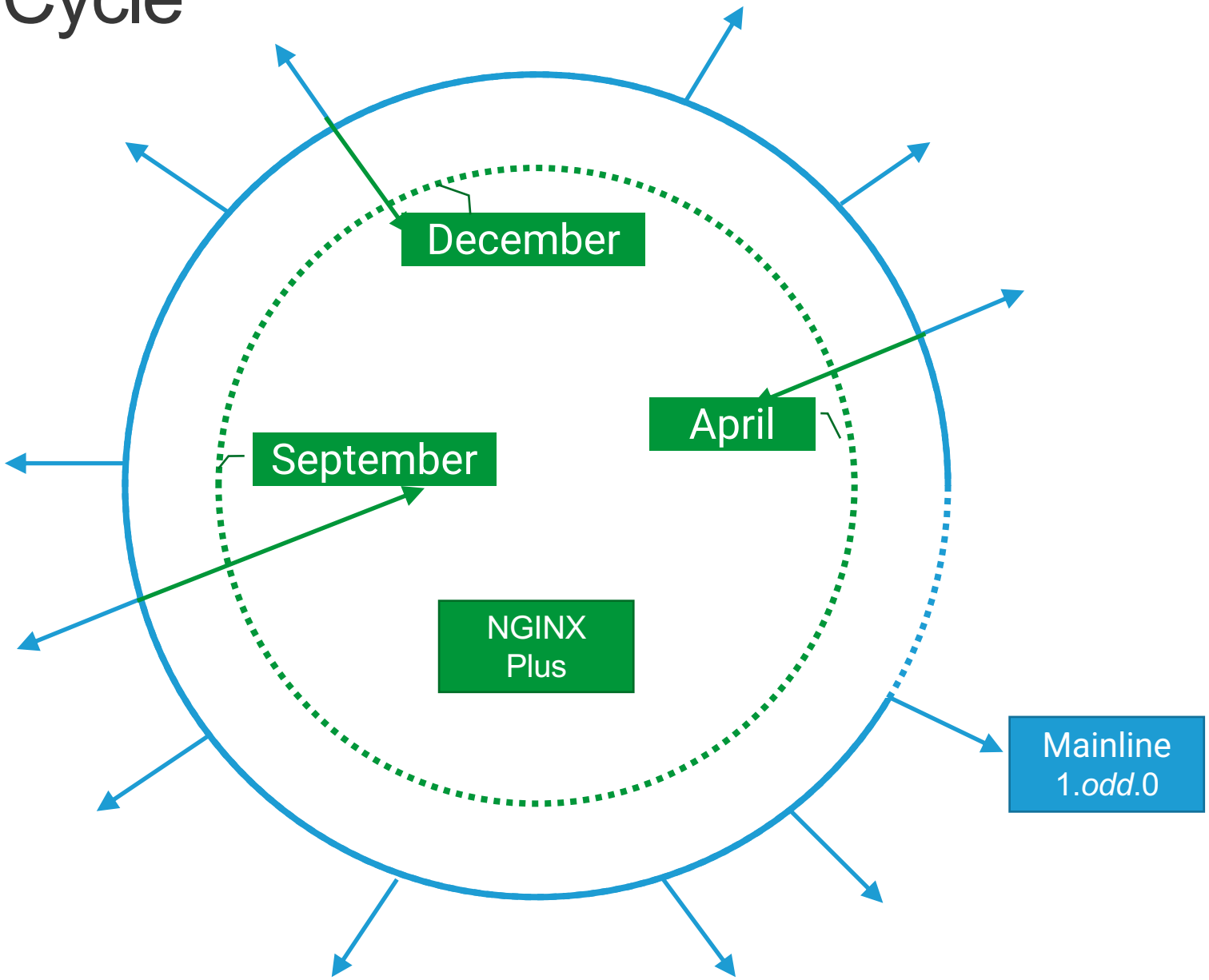
Выпуски NGINX за год



NGINX Open Source Cycle



NGINX Plus Cycle



2016

- Dynamic modules, incl. customer repo
- JWT authentication
- UDP load balancing
- JavaScript module

2017

NGINX+

- NGINX WAF
- All-new NGINX Plus API (fully RESTful)
- In-memory key-value store (API driven)
- Mirror requests

NGINX+

- HTTP/2 server Push & gRPC support
- OpenID Connect support
- State sharing across a cluster
  - Rate limiting, key-value store, sticky sessions
- Random w/ 2 choices load balancing

2019

NGINX+

- Dynamic certificate loading (from keyval)
- Observability enhancements
  - More metrics: per-location, per resolver, rate limits, connection limits, cluster status
  - Prometheus module
- Dry run modes (rate limits, connection limits)

2020

- Production-grade gRPC: dynamic routing, active health checks
- OpenID Connect maturity: multiple IdPs, PKCE support
- Unprivileged user installation

NGINX Controller

Сложности обеспечения работы приложений

Привязка к инфраструктуре

Ограничивает переносимость приложений

Изменения архитектуры приложений

Разработчики и DevOps переходят от «традиционных» виртуализированных сред к контейнерам и микросервисам

Узкие места сети и безопасности

Не позволяет появиться гибкости и сотрудничеству между командами

Плохая видимость состояния

Увеличивает проблемы (из-за ограниченного набора инструментов), связанных с управлением

Разрастание инструментария

Приводит к сложности и увеличению затрат

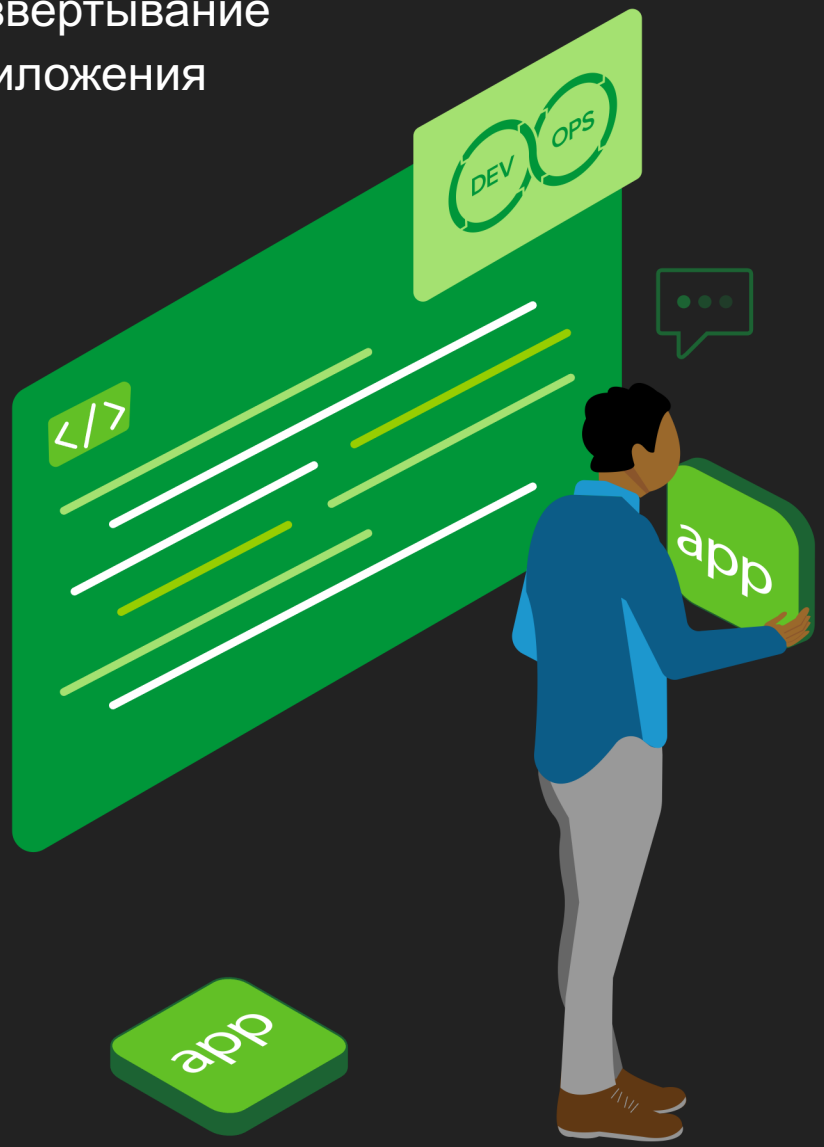
Зоны ответственности

Приходится брать на себя не свойственные обязанности

Отсутствие возможностей автоматизации и самообслуживания

DevOps

Развертывание
Приложения



NetOps

Погрязли в заявках

DevOps

Развертывание
Приложения

NetOps

Погрязли в заявках

DevOps

Развертывание
Приложения

NetOps

Погрязли в заявках

Сотрудничество, самообслуживание и автоматизация с помощью NGINX Controller

DevOps самостоятельно развертывает новое приложение

NetOps обеспечивает защиту и поддержку DevOps

Pain points

The market

- Proliferation of architectures
- The same vulnerabilities (for example injection, cross-site scripting) continue to exist after 20 years of application security best practices
- Organizations lack consistent policy to manage the growing complexity and risk of managing/tuning application security
- Cost of security breaches, downtime → lost revenue + CSAT impact

Application development

- Development has transformed to agile while security largely remains a manual effort
- Developers and DevOps outnumber security professionals by as much as 100:1
- Time-to-market pressure, friction between AppDev/DevOps and SecOps, and perception of security as a bottleneck results in poor testing, process, oversight

Pain points

SecOps

- Understaffed and struggle to keep up with rapidly changing threats
- Business leaders consider *compliance* versus *security* the goal
- Tool sprawl and inconsistent security policies spanning multiple architectures and clouds creates risk

DevOps

- Security slows down the application lifecycle and is perceived as a bottleneck
- CI/CD pipelines that automate app development/deployment lack security
- Business imperatives and incentives such as time to market compel DevOps to bypass SecOps. DevOps KPIs do not include security-related metrics

AppDev

- Developer training on security is lacking
- Developers are focused on modern app development and are not able to stay abreast of the security landscape
- Cloud and open source software introduce unknown risks to the business

Соединение разделенных SecOps и DevOps

Руководство

- Сопровождение и обучение
- Сделано для SecOps и для DevOps

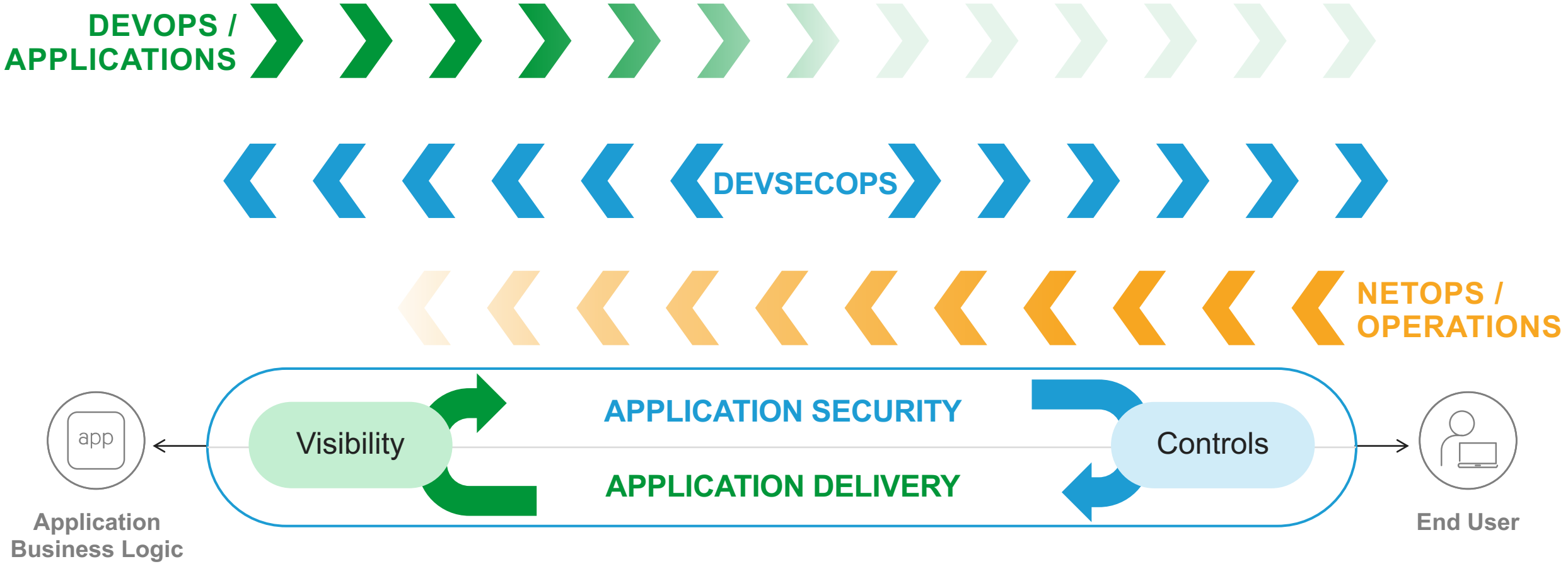
Управление

- SecOps все еще нужно определить политику
- Внесите туда свой опыт и установите правила

Ограничения

- Руководство для DevOps для обеспечения безопасности
- Но все же обеспечить гибкость

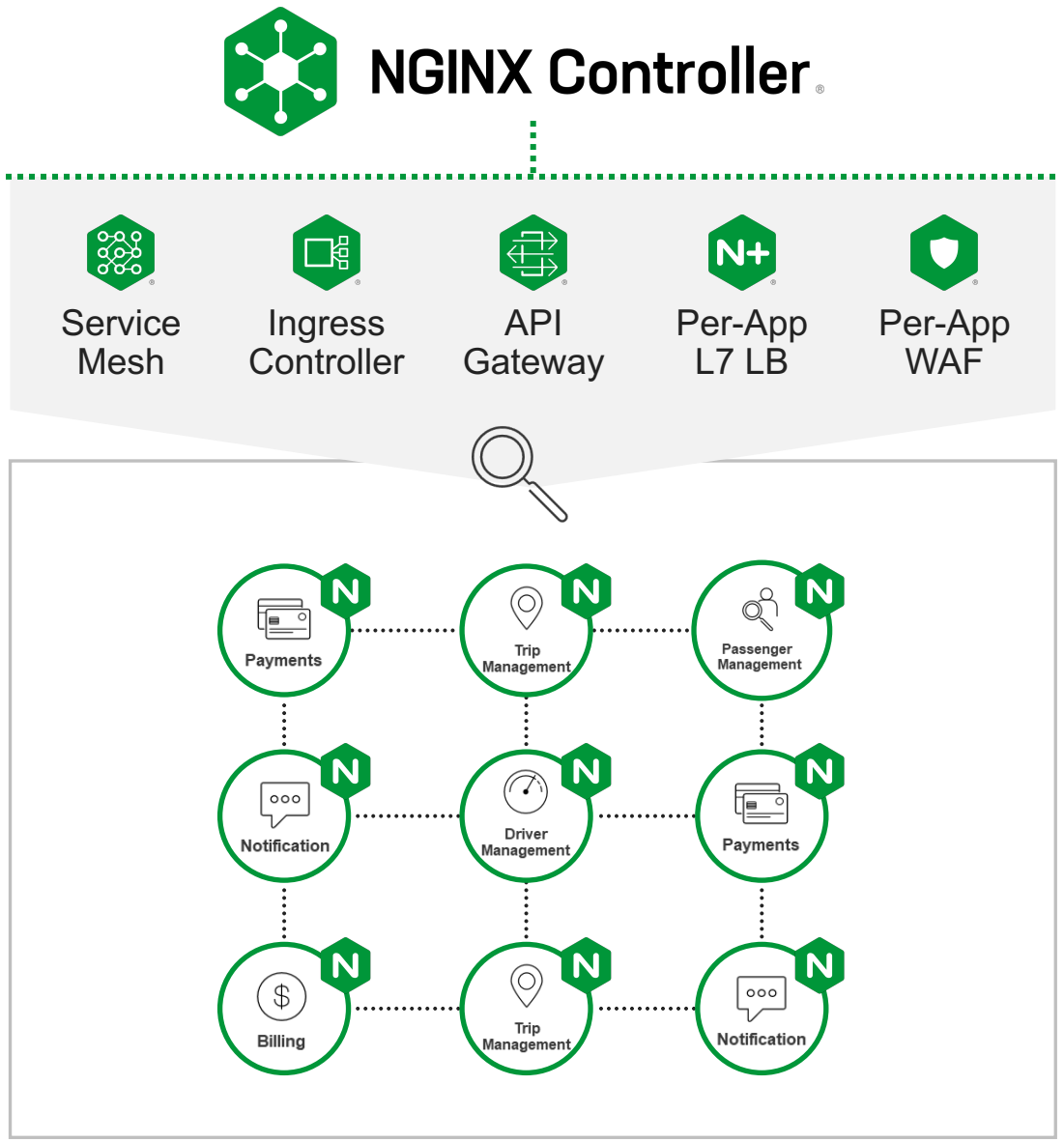
App services must include both **app delivery** and **app security**, which reinforce each other through visibility and controls



More easily embed security along the data path

Apply policies and controls consistently

Visibility across app services



NGINX Controller **автоматизирует** прикладной подход infrastructure-as-code

Decentralized, best-of-breed tools that developers need for **agility**…

…managed centrally to **simplify operations and security**…

… accelerating time-to-market **without introducing complexity.**

Controller App Delivery capabilities

SELF-SERVICE, AUTOMATION, AND REAL-TIME MONITORING

Self-service for DevOps

Empower DevOps teams to deploy and manage NGINX load balancers

- Role-based access control
- Self-service portal
- Implement blue-green and canary deployments with ease
- Auto deploy NGINX load balancers into AWS and Microsoft Azure
- Built on a distributed, cloud-native architecture – no limits on bandwidth or latency
- Lightweight, resulting in fewer components and lower TCO

Automate app delivery

Integrate NGINX deployment and configuration into DevOps workflows

- API first - RESTful configuration
- CI/CD integration
- Deploy and maintain using Ansible

App-centric user interface

Eliminate need to stitch together end-to-end view by abstracting infrastructure

- Define and configure policies on a per-app basis
- Monitor health of entire application
- Troubleshoot apps quickly

Real-time monitoring and alerting

Get critical insights into application performance

- Visualize and alert on more than 200 metrics
- Forward metrics and alerts to Datadog and Splunk
- Retrieve metrics using APIs

Controller App Security

Bridge the divide between DevOps and SecOps teams

- Deploy WAF for app protection and threat visibility
- Reduce time and effort fixing security issues by integrating WAF into DevOps workflows
- Out-of-the-box OWASP Top 10 protection

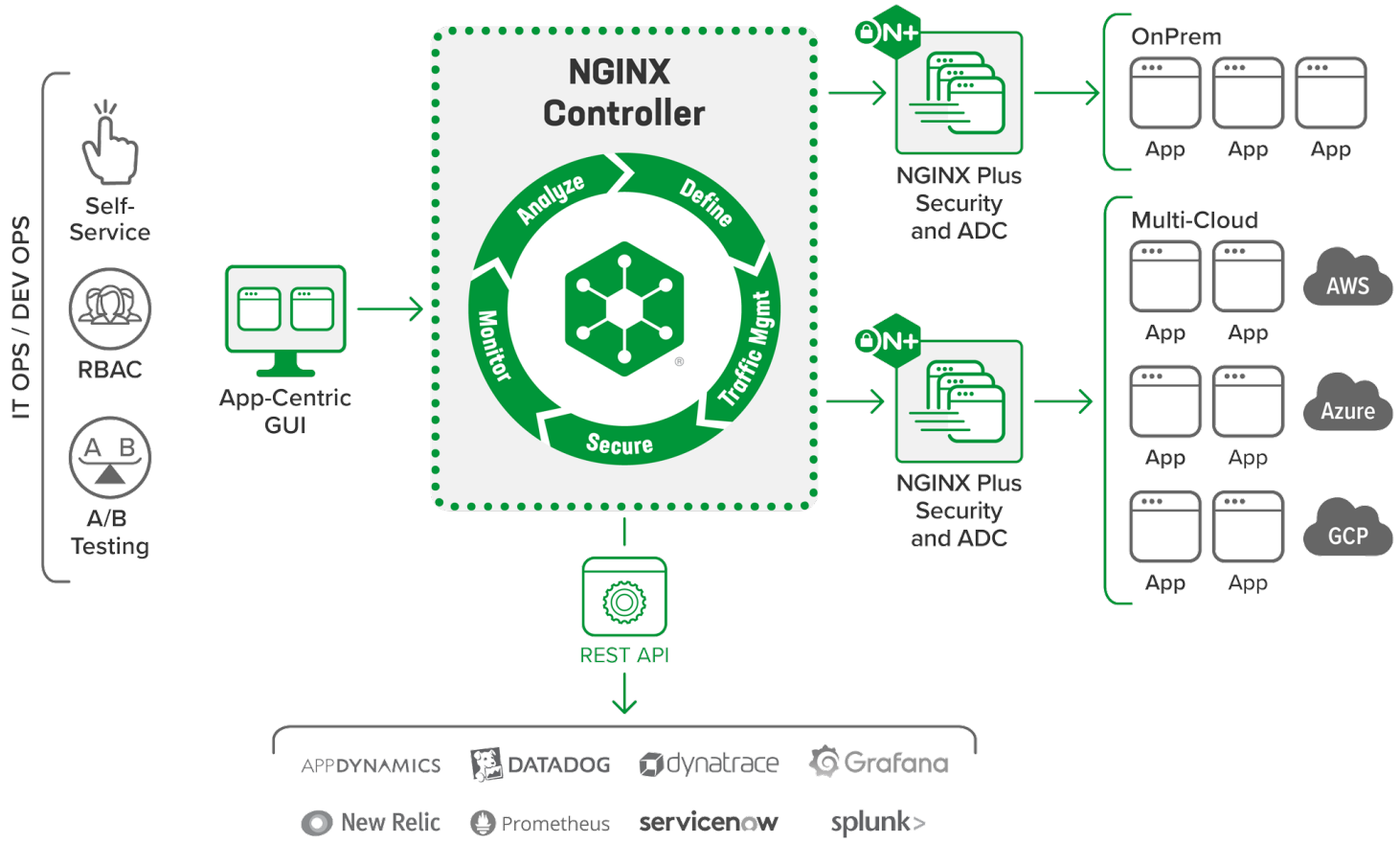
Certificate management

Boost productivity using built-in certificate manager

- Save time and effort by managing all your certificates using a centralized interface, APIs, or both
- Get notified about expired certificates

Самообслуживание для DevOps

ПРЕДОСТАВЬТЕ КОМАНДАМ DEVOPS ВОЗМОЖНОСТЬ РАЗВЕРТЫВАТЬ NGINX И УПРАВЛЯТЬ ИМИ

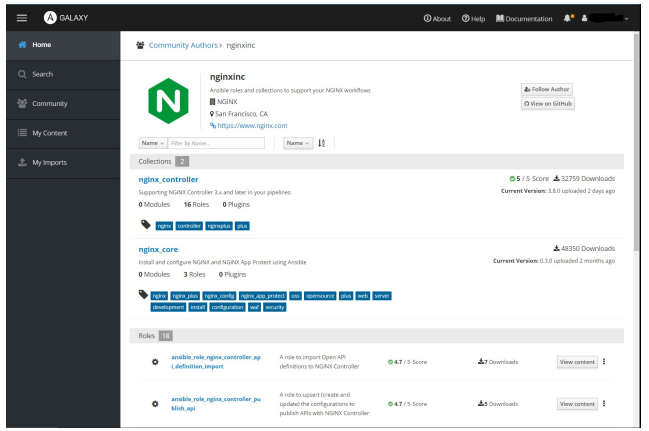


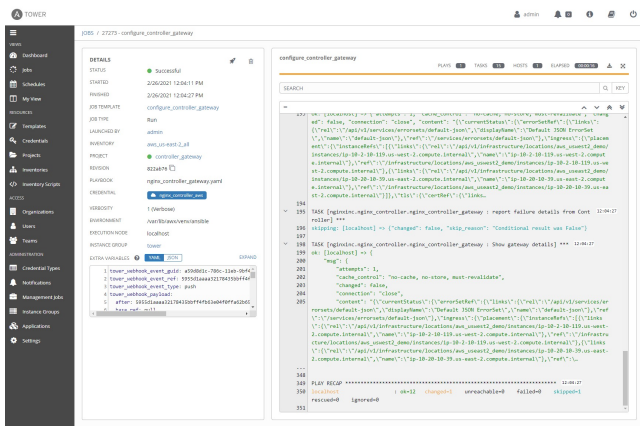
- Устранение узких мест с помощью портала самообслуживания
- Обеспечение соответствующих разрешений для нужных пользователей с помощью управления ролевым доступом
- С легкостью реализуйте сине-зеленые и канареечные развертывания, чтобы создавать лучшие приложения
- Автоматическое развертывание NGINX в средах AWS, Azure и VMware
- Неограниченная пропускная способность и минимальная задержка с помощью распределенной облачной архитектуры

Автоматизированная доставка приложений

ИНТЕГРИРУЙТЕ РАЗВЕРТЫВАНИЕ И НАСТРОЙКУ NGINX В ПРОЦЕССЫ DEVOPS

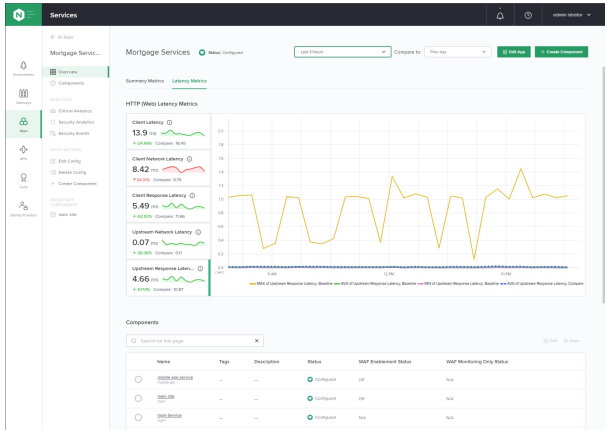
- Ускорение развертывания приложений и обеспечение повторяемости и стандартизации
- Настраивайте с помощью современного конфигурации RESTful API
- Автоматизация подготовки и развертывания доставки приложений и безопасности NGINX
- Интеграция доставки приложений с конвейерами CI / CD и системами автоматизации
- Развертывание и поддержка NGINX с помощью Ansible

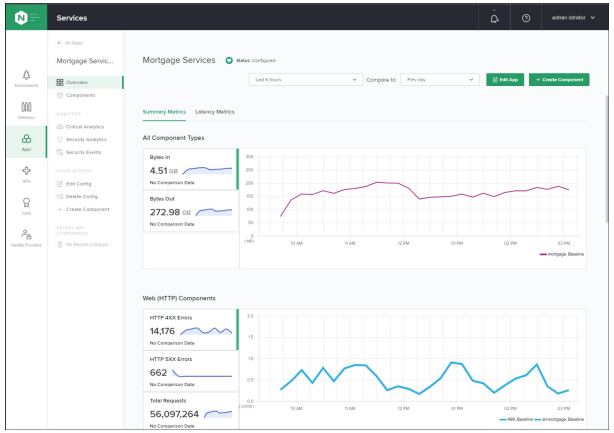


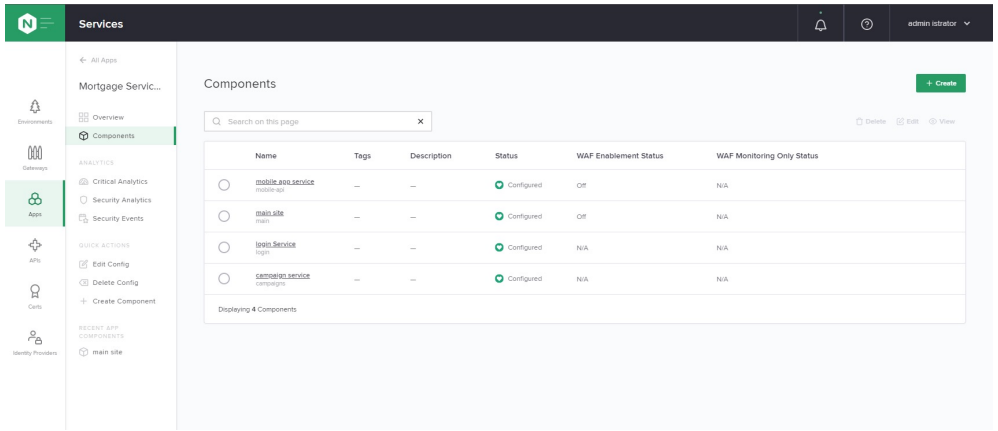


Интерфейс, ориентированный на приложения

УПРОЩАЙТЕ РАБОТУ С ПОМОЩЬЮ МОНИТОРИНГА И УПРАВЛЕНИЯ ОРИЕНТИРОВАННОГО НА ПРИЛОЖЕНИЯ





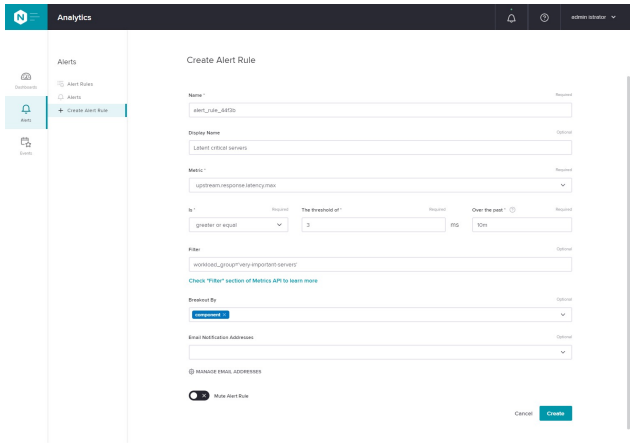


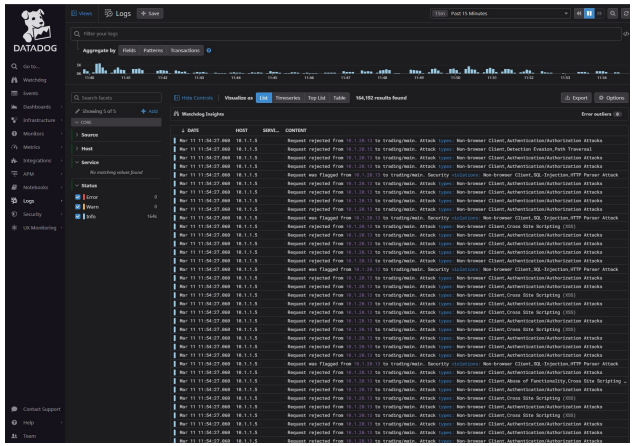
- Сосредоточьтесь на приложении, а не на инфраструктуре
- Определяйте и настраивайте политики для каждого приложения
- Упростите и оптимизируйте поиск проблем, чтобы сократить MTTI и MTTR
- Сохраняйте прозрачность важных показателей приложения: задержка, ошибки 4XX и 5XX, запросы и байты.
- Оптимизируйте производительность приложений и выявляйте проблемы с помощью аналитики по каждому приложению

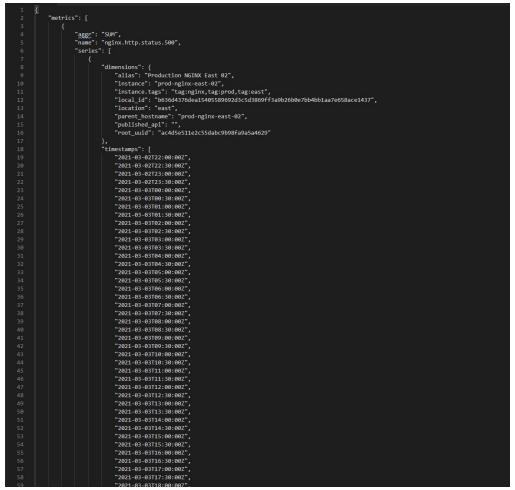
Мониторинг и оповещение в реальном времени

ПОЛУЧИТЕ ПРЕДСТАВЛЕНИЕ О ПРОИЗВОДИТЕЛЬНОСТИ ПРИЛОЖЕНИЙ

- Держите руку на пульсе своих приложений и инстансов NGINX Plus
- Мониторинг и получение предупреждений для более чем 200 показателей работы приложений и пороговых триггеров
- Воспользуйтесь другими инструментами мониторинга и аналитики, такими как Splunk или Datadog для еще большей прозрачности
- Создавайте и настраивайте правила предупреждений на основе определенных показателей приложения.
- Получение аналитики через графический интерфейс или API

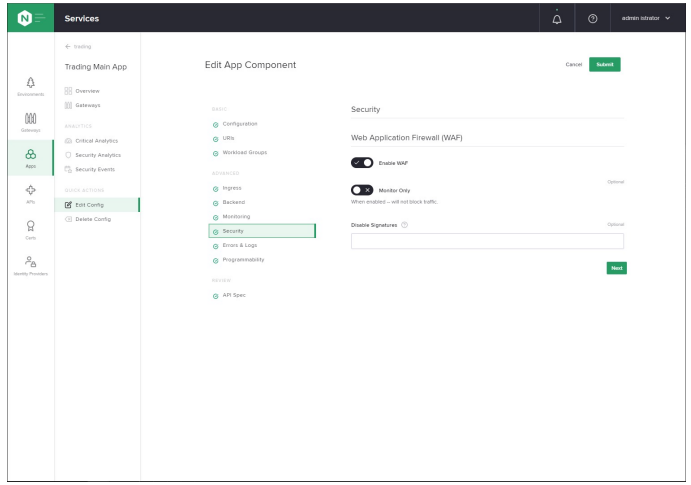


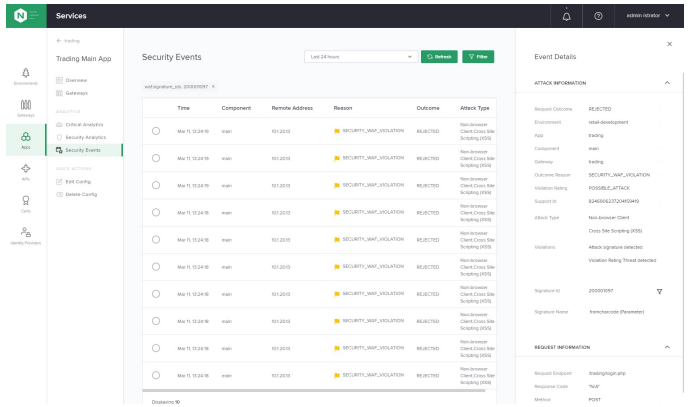




Безопасность приложений

ПРЕОДОЛЕТЬ РАЗРЫВ МЕЖДУ КОМАНДАМИ DEVOPS И SECOPS



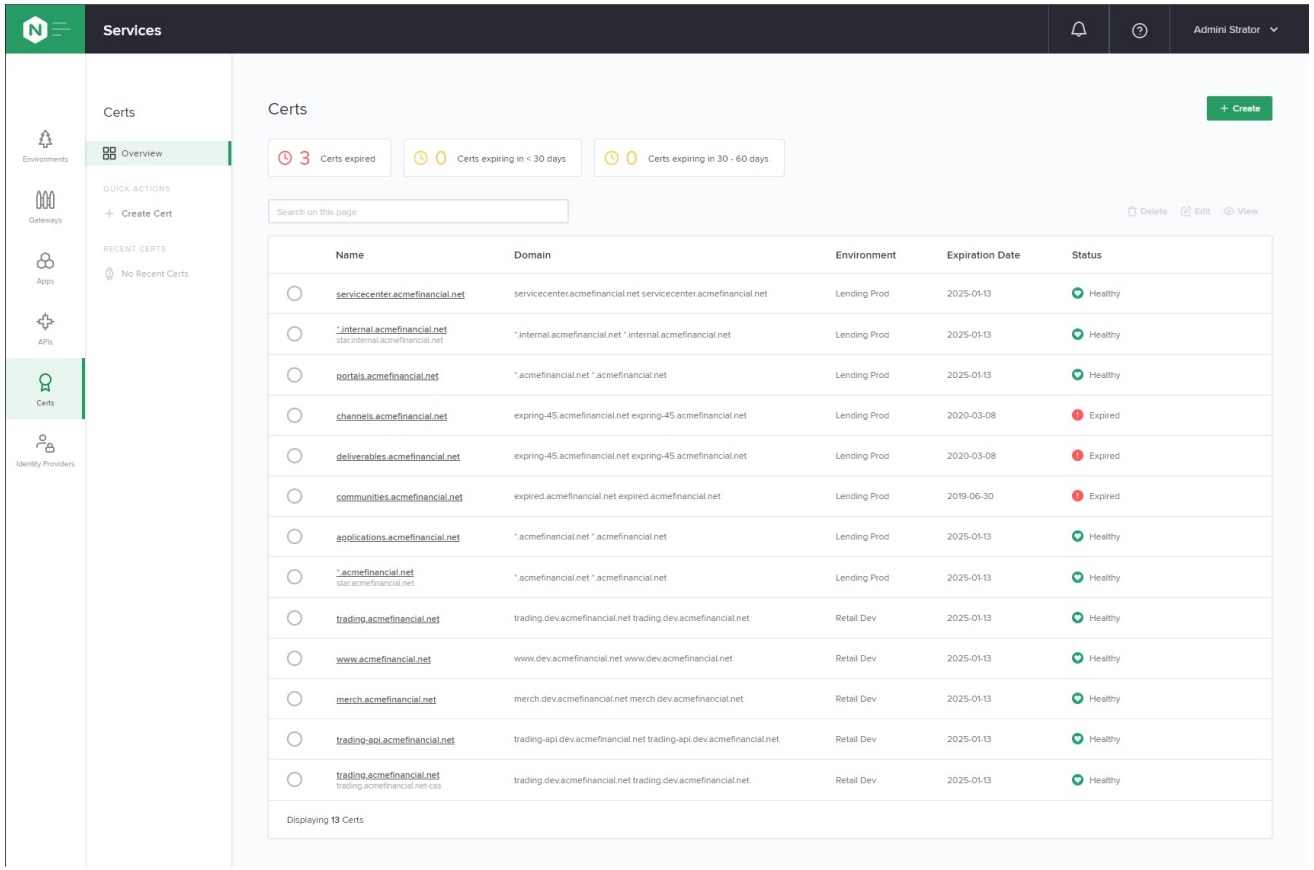


- Унифицируйте операции по доставке приложений и управлению безопасностью
- Определяйте и настраивайте службы и политики безопасности для каждого приложения
- Убедитесь, что защита включена в процесс разработки и развертывания приложения
- Добавление политик безопасности через графический интерфейс или API
- Получите готовую защиту от распространенных векторов атак, включая OWASP Top 10

Управление сертификатами

ПОВЫСЬТЕ ПРОИЗВОДИТЕЛЬНОСТЬ С ПОМОЩЬЮ ВСТРОЕННОГО МЕНЕДЖЕРА СЕРТИФИКАТОВ

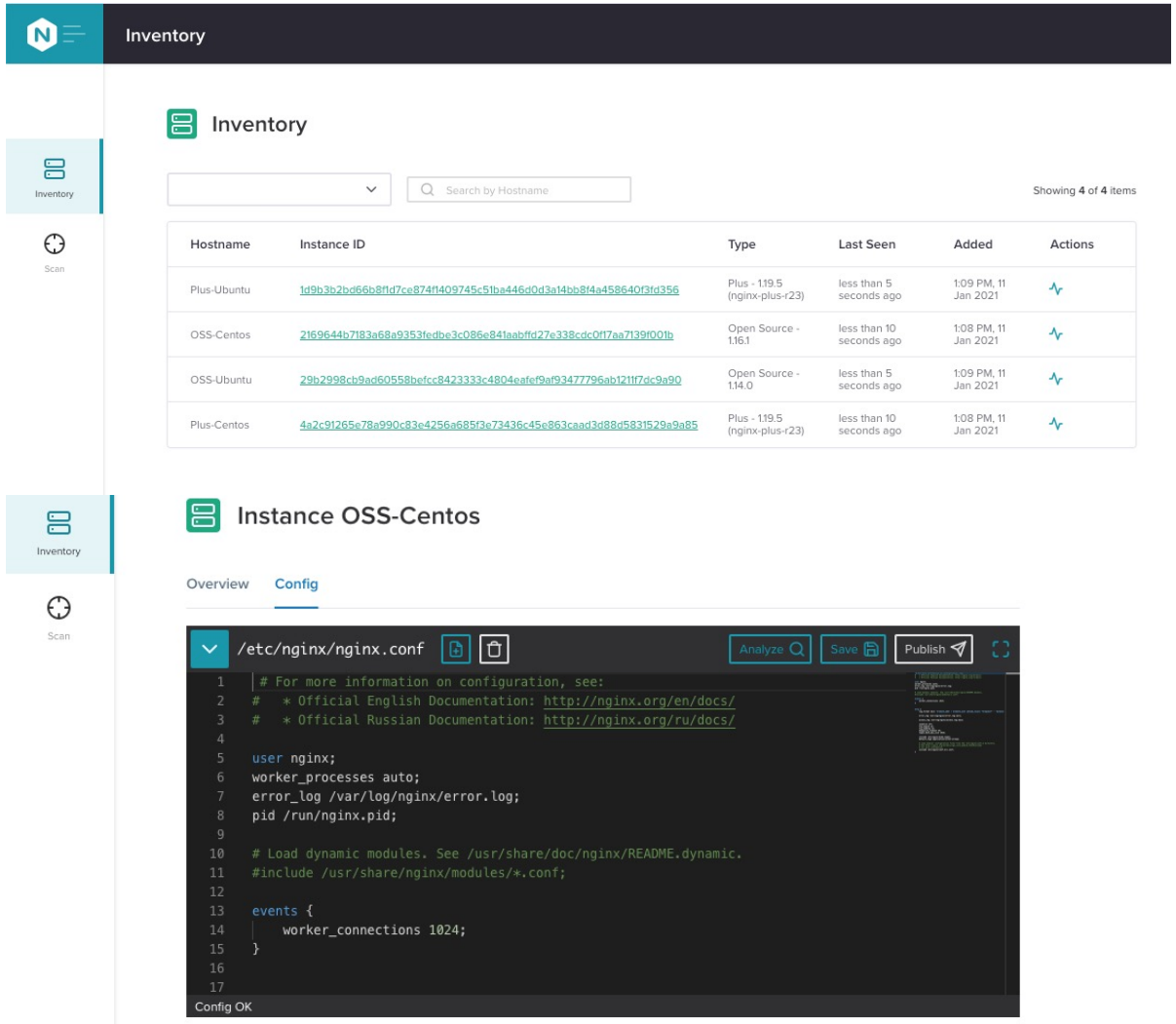
- Избегайте дорогостоящих и длительных простоев из-за сроков действия сертификатов
- Создание сертификатов через графический интерфейс или API
- Централизованное управление сертификатами NGINX plus для каждой среды
- Получайте информацию о сертификатах с истекшим сроком или о тех, срок действия которых скоро истечет
- Загрузите сертификаты из предпочитаемого центра сертификации



NGINX Instance Manager

Обзор

NGINX INSTANCE MANAGER



Простота

- Настраивает и поддерживает инстансы NGINX в нужном вам количестве
- Читает существующие файлы conf
- Работает с вашими существующими конфигурациями, инструментами и процессами
- Лучшая статистика
- Приоритет API First
- Метрики представляются на Prometheus Query Language

Найдите и защитите инстансы

- Сканирование с использованием скрытых портов и тегов
- CVE-уязвимости и информация об устаревших версиях
- Обнаружение и замена сертификатов с истекшим сроком

Управление конфигурацией

- Централизованная проверка
- Анализ и предложения
- Легкий пользовательский интерфейс управления инмстансами
- Уведомление об откате и изменении (скоро будет)
- Шаблоны для публикация в нескольких экземплярах по тегам

Основные возможности

Поиск и обнаружение инстансов

Управление конфигурацией

Метрики и оповещения во вне системы

API для NGINX Instance Manager

Управление сертификатами

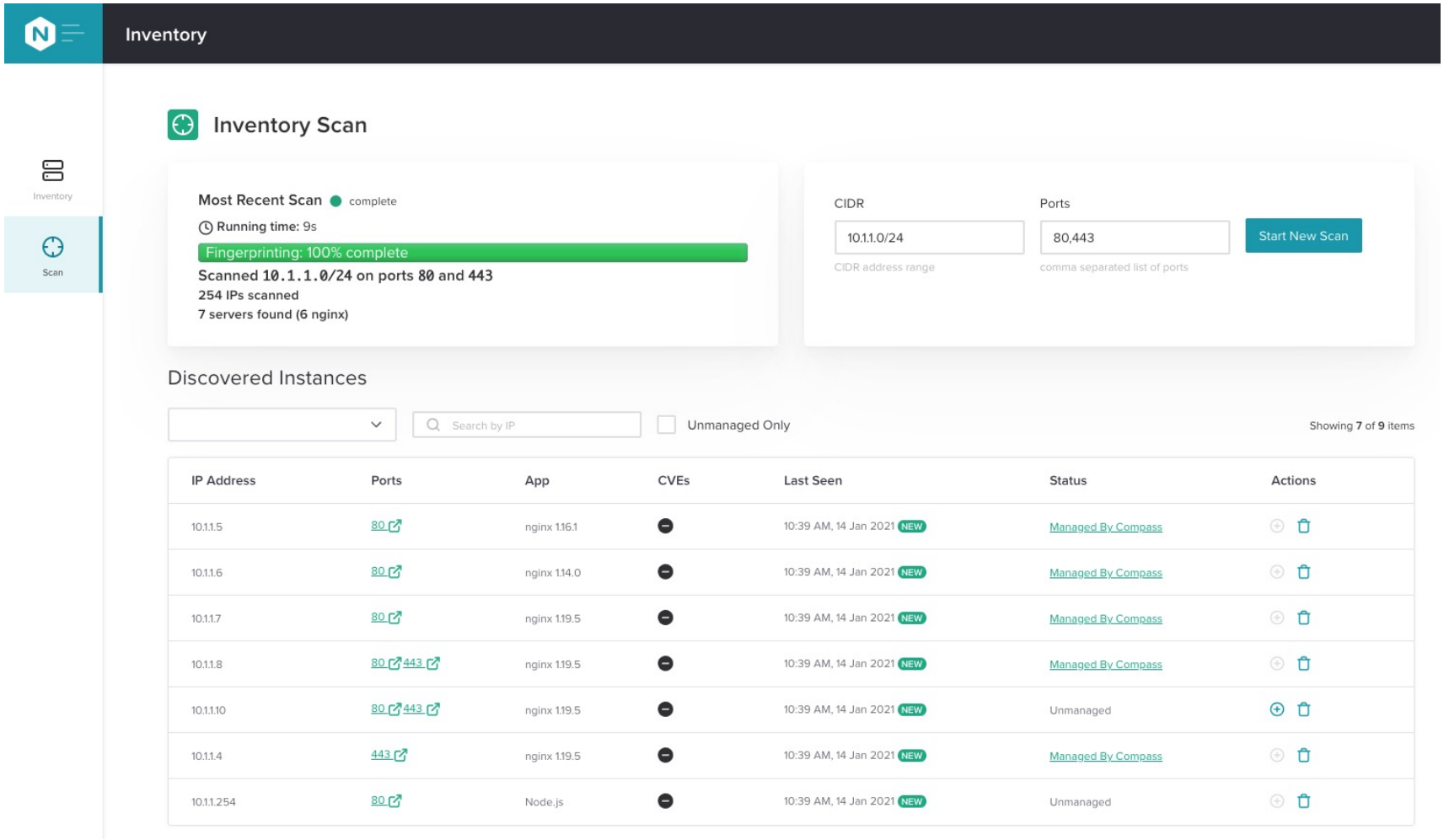
Тегирование

Совместимость с существующими интсрументами

Простая установка как Linux Service из пакета

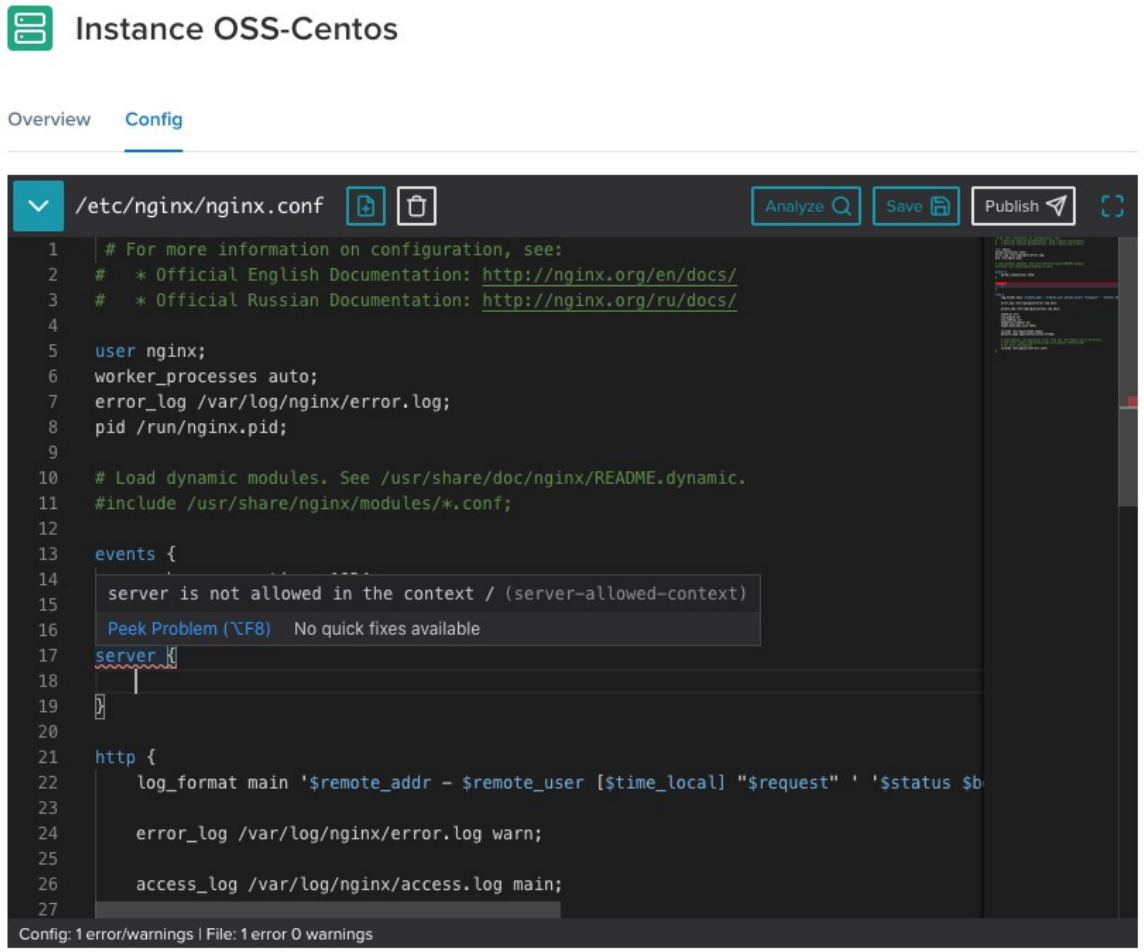
Поиск и обнаружение инстансов

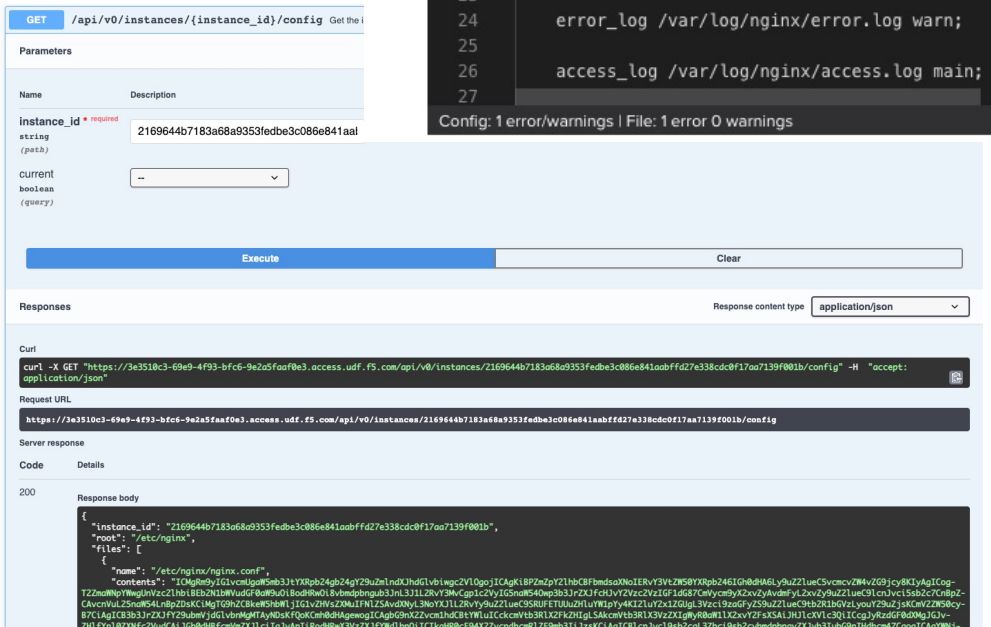
- Nmap технология скрытого сканирования
- Определяет тип сервера
- Выдаёт списокCVE list
- Запускается по требованию через API



Configuration Management

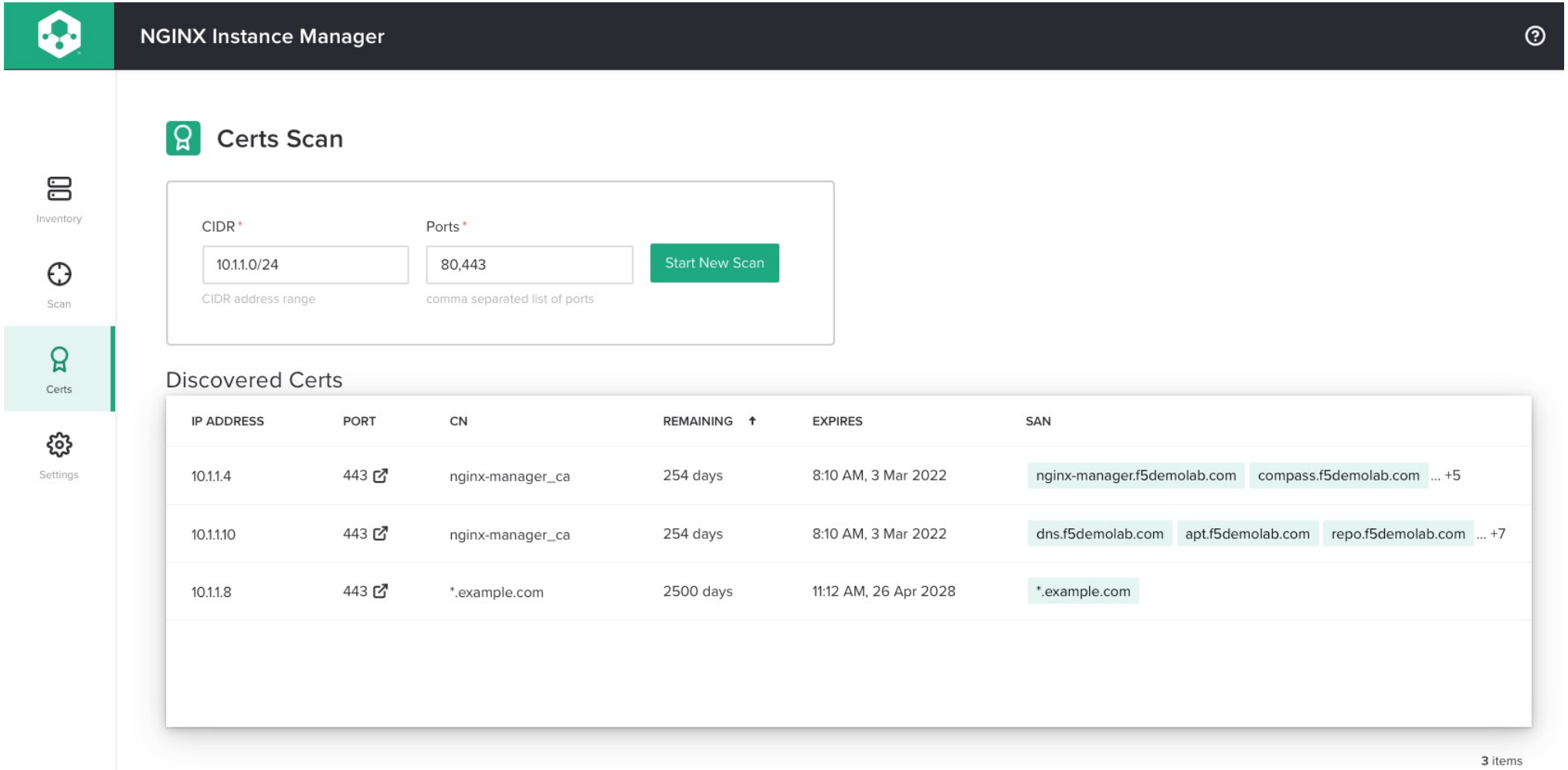
- Analyzer Functionality for finding errors.
  - Built-in editor
- Native VisualStudio Code format
- API
  - GET/PUT multiple includes
- Add/Delete files in conf from Compass





Сканирование истекших сертификатов

БЕЗ ИСПОЛЬЗОВАНИЯ АГЕНТА!



Замена сертификатов

ОТПРАВЛЯТЬ ДРУГИЕ ФАЙЛЫ В NGINX ЧЕРЕЗ UI ИЛИ API

Plus-Centos

/etc/nginx/conf.d/example.com.conf

```
40    # ww2.example.com HTTPS
41    # See best practices for security and compatibility here: https://
42    server {
43        listen 443 ssl;
44        status_zone www2.example.com_https;
45        ssl_certificate /etc/ssl/example.com.crt;
46        ssl_certificate_key /etc/ssl/example.com.key;
47        server_name ww2.example.com;
48        location / {
49            include includes/proxy_headers/proxy_headers.conf;
50            proxy_pass http://dummy_servers;
51        }
52
```

Upload Files

This tool allows you to upload related files that aren't part of the nginx config. Files uploaded here will be immediately pushed to the instance.

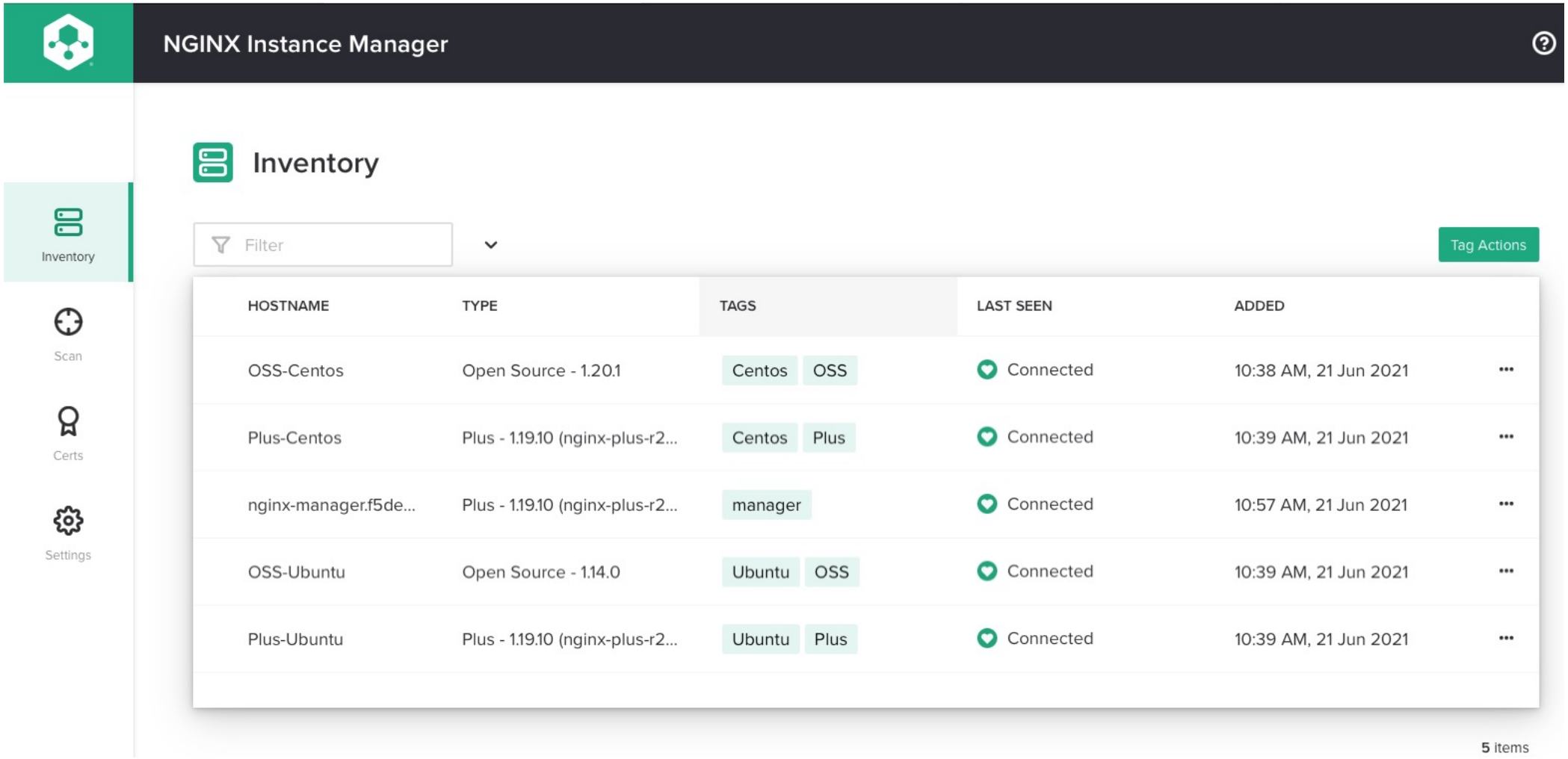
/etc/ssl/example.com.crt

Paste file contents here...

Upload

Новый пользовательские интерфейс

РАБОТА С БОЛЬШИМ КОЛИЧЕСТВОМ ИНСТАНСОВ С ПОМОЩЬЮ ТЕГОВ



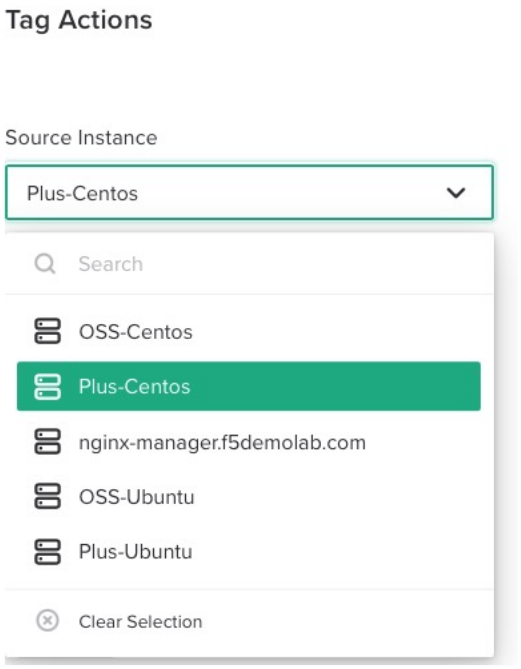
Tag Your Environment

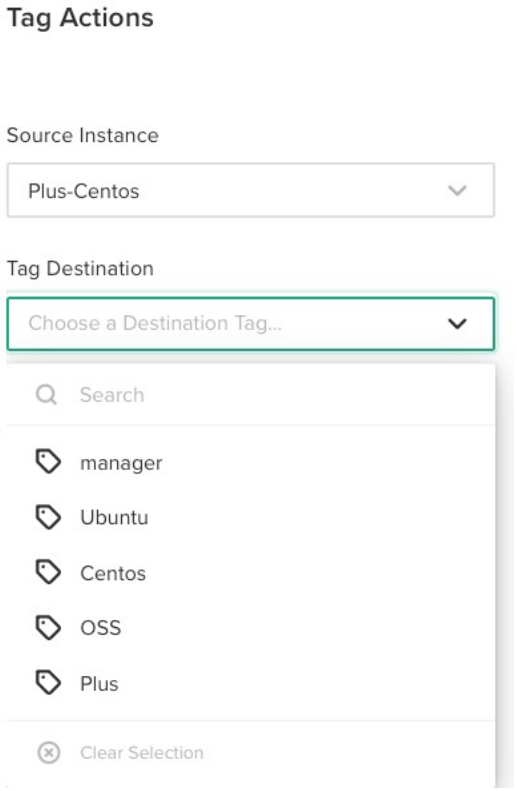
HANDLE LARGE NUMBERS OF INSTANCES USING TAGS

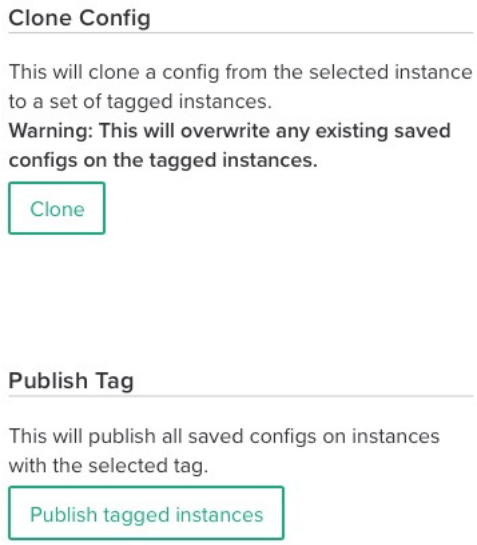
- Powerful way to organize and manage your configurations
- Categorize instances based on person, purpose, environment
- Filter views by Tags
- Standardize configurations based on tags

Клонирование конфигураций

ПРИМЕНЕНИЕ КОНФИГА НА ВСЕ ИНСТАНСЫ С УКАЗАННЫМ ТЕГОМ







Roles

MATCH TAGS TO USERNAMES WITH OPENID CONNECT

Roles consist of matching:

- username
- one or more tags
- role type (Full Admin, Read/Write, Read Only).

Full Admins can see all tags

Read/Write and Read Only can only see instances with the tags in the role.

Отправка метрик

Отправляет данные:

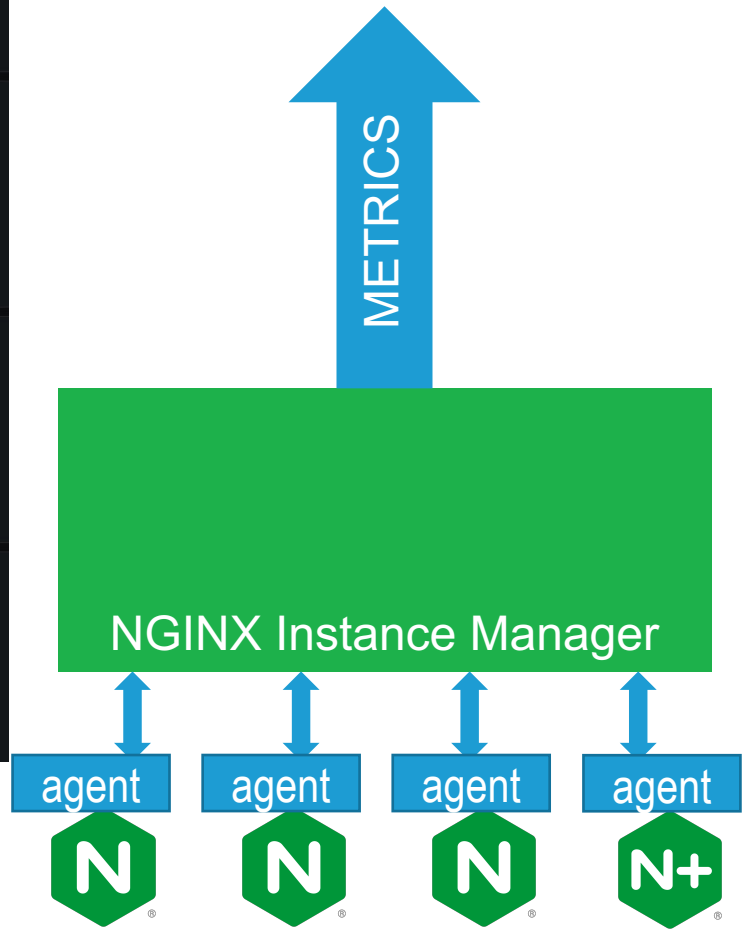
- Analytics as a Service
- Grafana/Prometheus

Настроить оповещения о существующих инстансах.

Предоставляет все метрики NGINX Plus и OSS

Prometheus

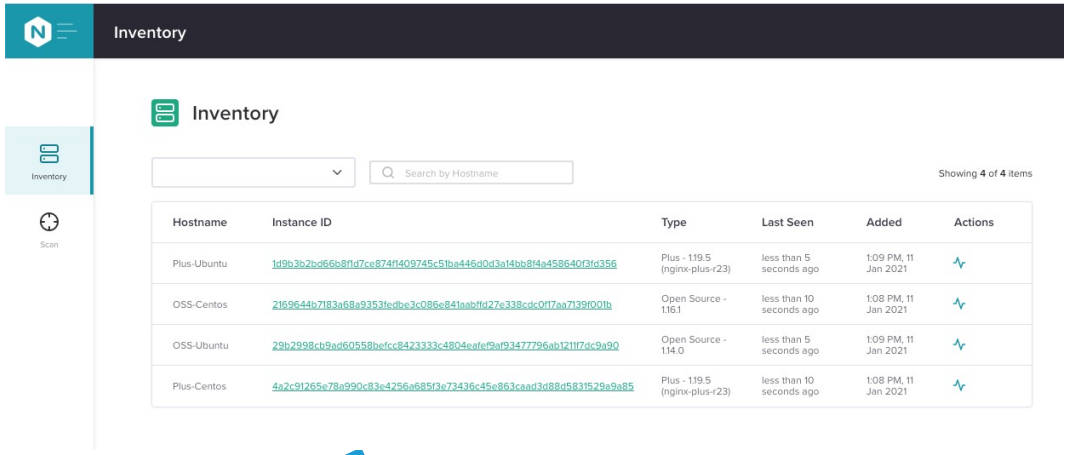
Grafana



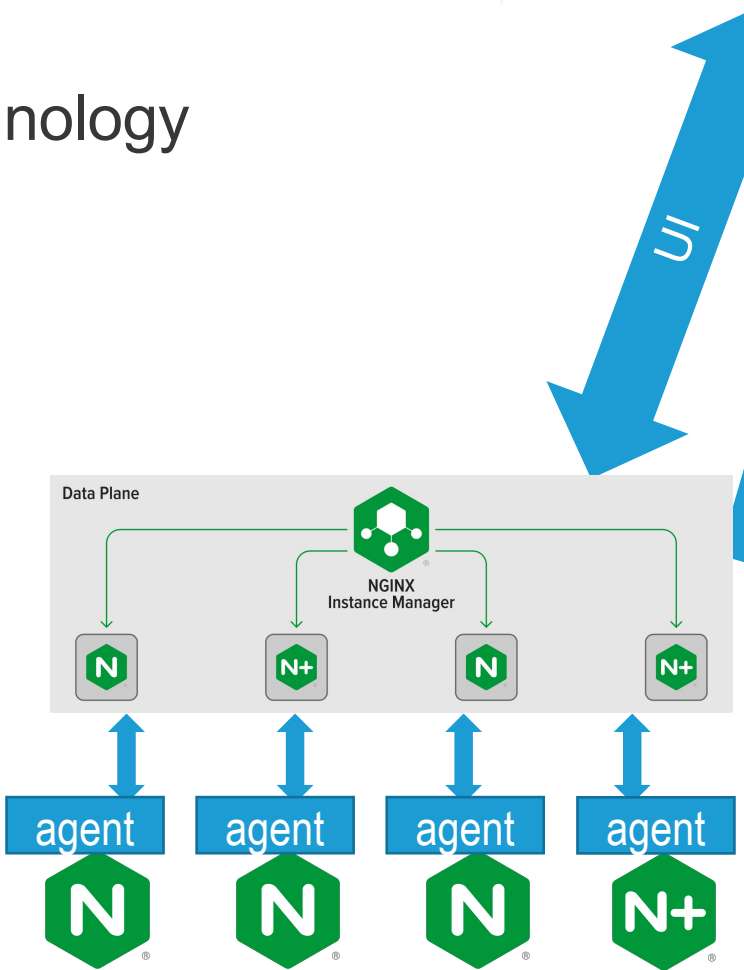
API for NGINX

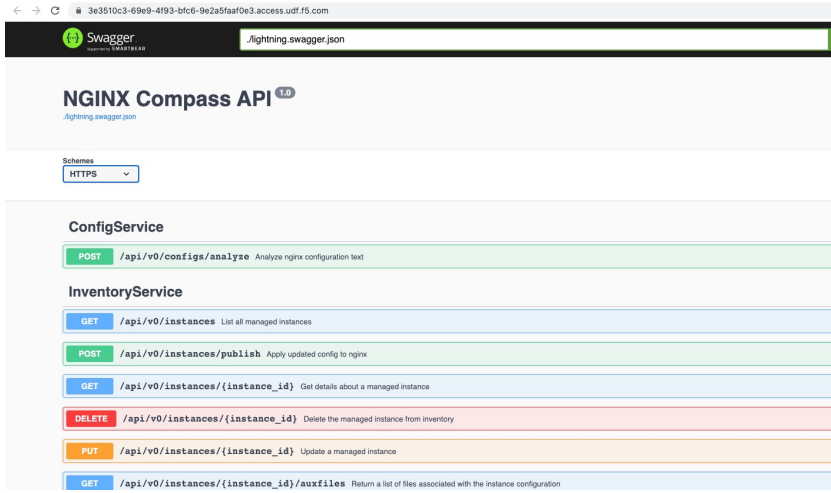
Simple RESTful API

- Declarative Based
- Uses NGINX terminology



UI for Ops/Demos





{ API }

API for AppDev
CI/CD
Automation

Элементарная установка

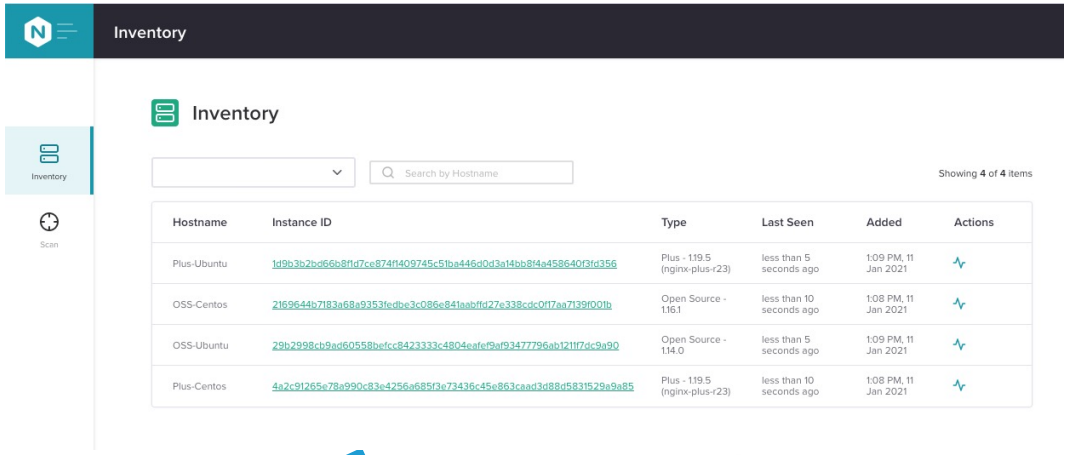
- Установка и запуск за секунды
- Работает как служба Linux
- Обновления через yum/apt/dnf

```
NGINX-AGENT(8)                    BSD System Manager's Manual                    NGINX-AGENT(8)

NAME
     nginx-agent – Instance Management for NGINX; quick, fast and easy

SYNOPSIS
     nginx-agent [-h] [--flag argument]

DESCRIPTION
     nginx-agent ( pronounced "engine x" ) is an agent for NGINX.  The NGINX Agent is used by other NGINX
     programs to manage NGINX instances.  Like NGINX, the agent is known for its high performance, sta-
     bility, simple configuration, and low resource consumption.

     The options are as follows:

     -h, --help          Print help.

     --server address    Name and gRPC port of the server to connect to as address. IP address or FQDN
                         can be used.  The default address is "localhost:10000".

     --nginx.basic_status_url URL
                         NGINX Open Source stub_status page URL.  Example ("http://localhost:80/stub_sta-
                         tus").

     --nginx.plus_api_url URL
                         NGINX Plus API URL.  Example ("http://localhost:8080/api").
```

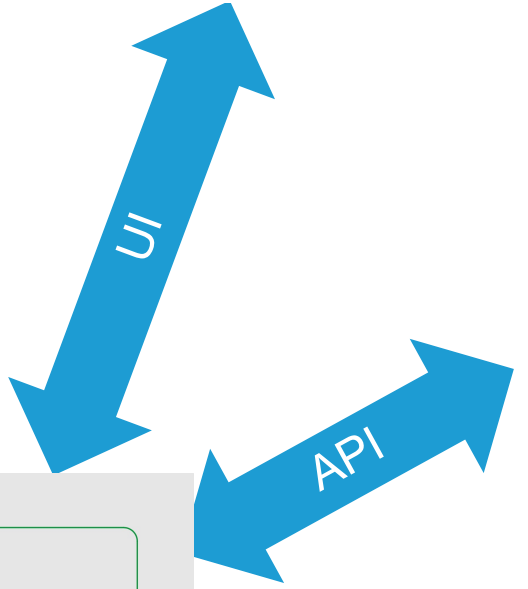
```
compass_0.0.1-2778301.x86_64.rpm                                        |  22 MB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating   : compass-0.0.1-2778301.x86_64                                              1/2
Platform systemd (default) detected. Installing service.
To start this service, use: systemctl start compass
---------------------------------------------------------------------

Thank you for using NGINX!

     Product: compass
     Version: 0.0.1
       Build: 2778301

Please find the documentation for NGINX compass here:
https://docs.nginx.com/nginx-compass/install/

NGINX compass is proprietary software. EULA and License information:
/usr/share/doc/compass/

For support information, please see:
https://www.nginx.com/support/

Configuration settings can be adjusted here:
/etc/compass/compass.conf

---------------------------------------------------------------------
  Cleanup    : compass-0.0.1-2772636.x86_64                                              2/2
  Verifying  : compass-0.0.1-2778301.x86_64                                              1/2
  Verifying  : compass-0.0.1-2772636.x86_64                                              2/2

Updated:
  compass.x86_64 0:0.0.1-2778301

Complete!
[centos@compass ~]$ systemctl status compass
● compass.service - compass
   Loaded: loaded (/etc/systemd/system/compass.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/compass.service.d
           └─override.conf
   Active: active (running) since Thu 2021-01-14 15:45:33 UTC; 41min ago
 Main PID: 975 (compass)
   CGroup: /system.slice/compass.service
           └─975 /usr/sbin/compass /usr/sbin/ngxscan
```

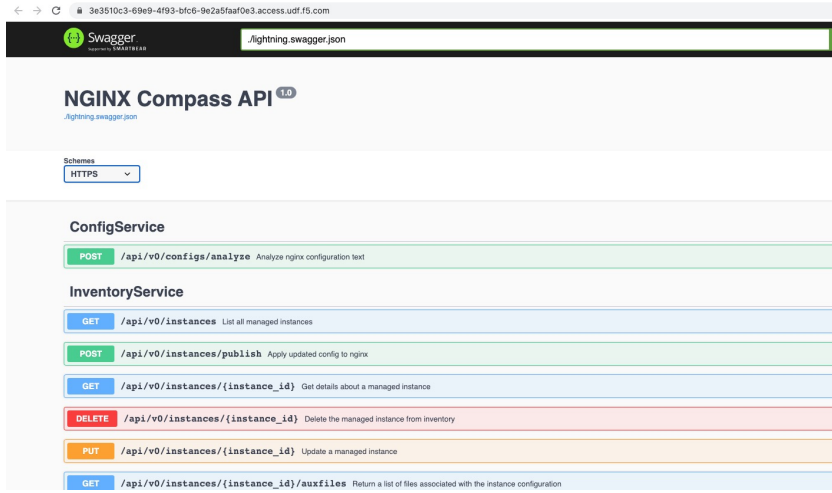
Совместимость с существующими процессами

- Работает с существующим конвейером (не действует как владелец конфигурации)
- Расширенные возможности по настройке Nginx Plus



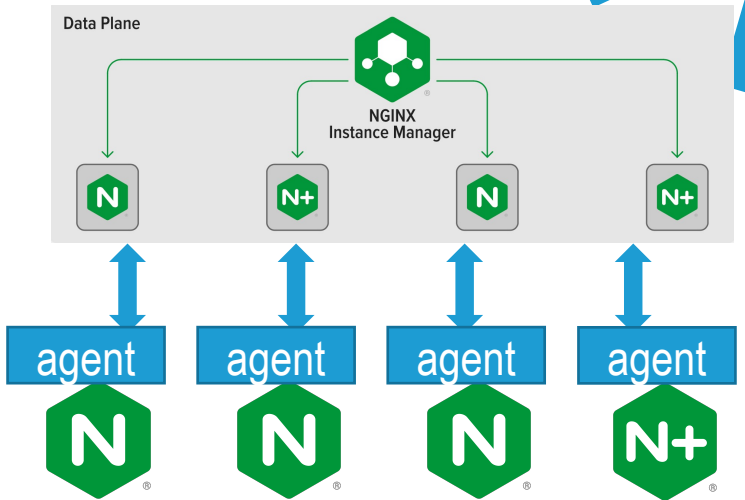
UI для Ops/Demos





{ API }

API для AppDev
CI/CD
Automation



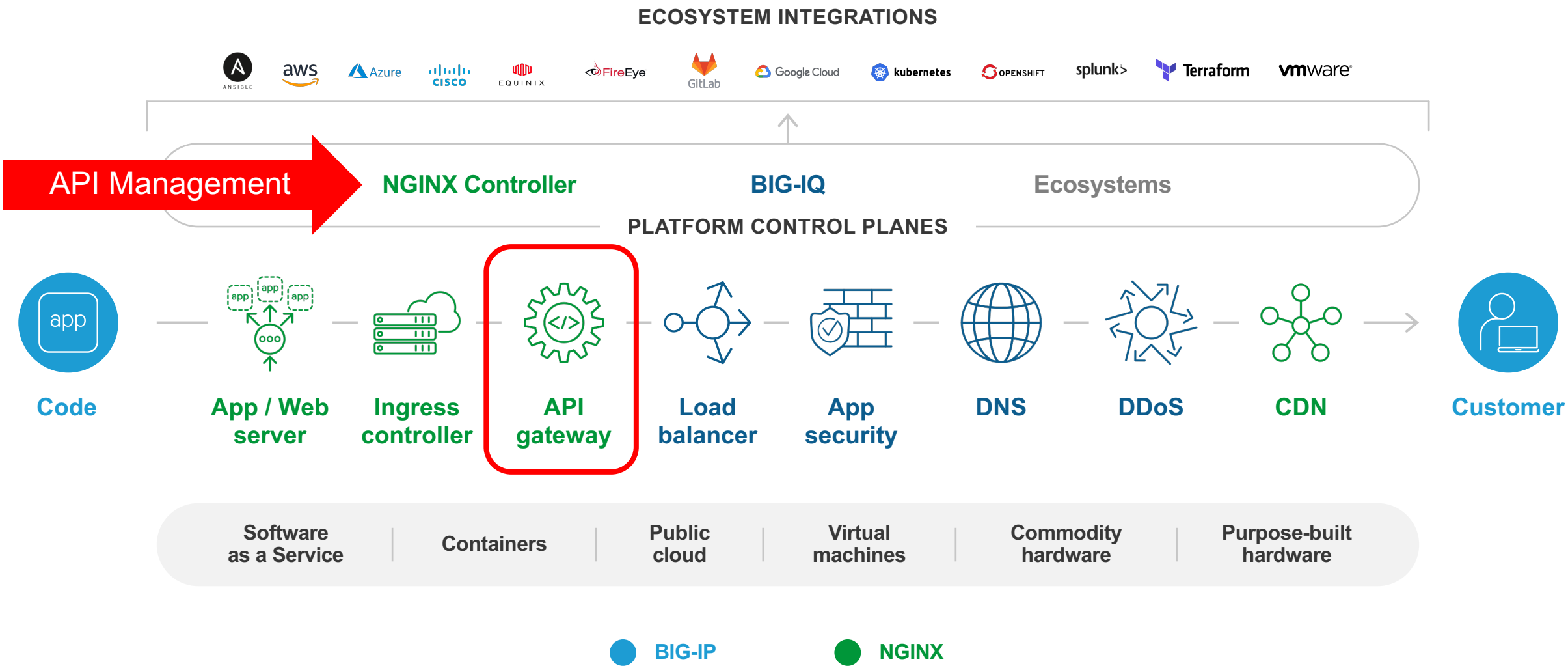
Instance Manager vs Controller

NGINX Instance Manager - для data plane первую очередь предназначен для сегодняшних пользователей Nginx.
NGINX Controller - для control plane предназначен для сложных и новых систем

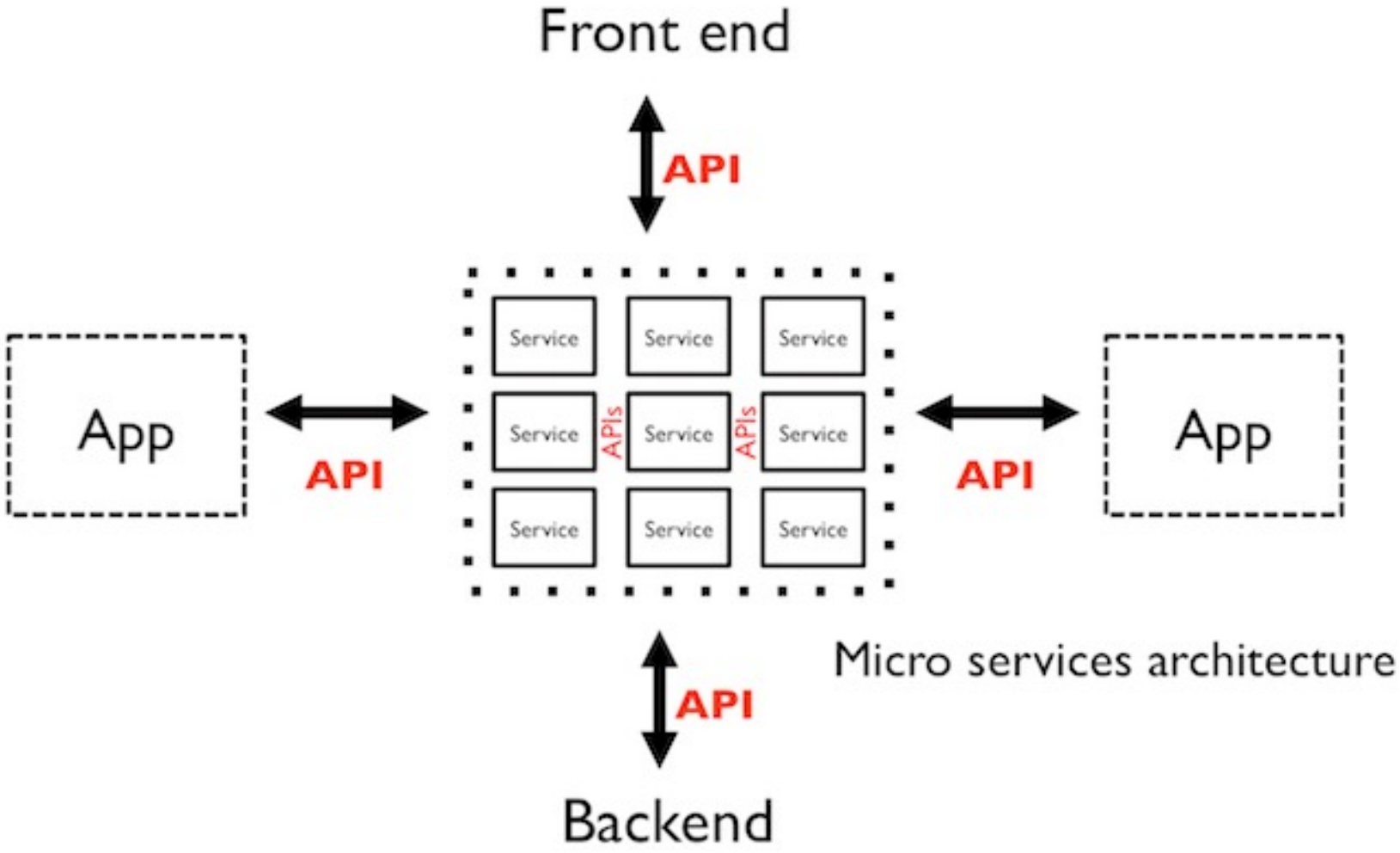
	Instance Manager	Controller
Target Persona	Dev, DevOps	NetOps, DevOps, API Owner, Cloud Architects
Target NGINX Users	Community (Open Source)	Greenfield NGINX Plus Opportunities
Delivery model	**Software**	**Software**
NGINX Config Management for NGINX experts AND NON Experts	✓	
Analyzer v2	✓	✓
Metrics	✓	✓
Role based access control	OpenID Connect	✓
Support for advanced use cases (APIM, App Protect & Service Mesh)		
Bundled data plane (consumption)		✓
Pricing	Contract SKUs (Instance Count)	Contract SKUs (App Counts)
API Support	Simple/REST	Full/Declarative-ISH

API Management

APIs: From Code to Customer



API – это основа современных микросервисных приложений



As apps are modernized, the adoption of microservices and APIs increases

52%

Organizations that use microservices concepts, tools, and methods for software development[1]

60%

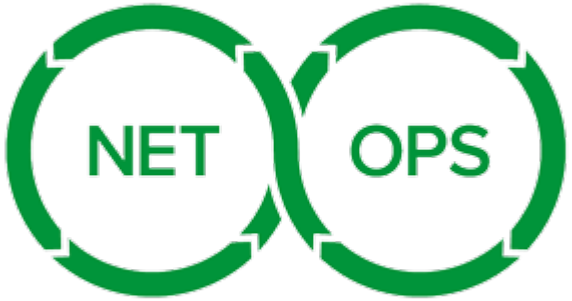
Enterprises running 50 or more microservices[2]

25%

Enterprises with over 1000 APIs, driven by the increased adoption of microservices[3]

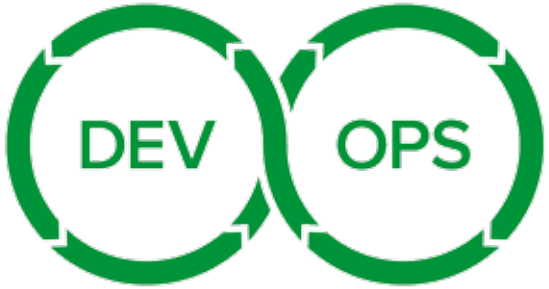
1) https://www.oreilly.com/radar/cloud-adoption-in-2020/
2) https://devops.com/survey-sees-massive-adoption-of-microservices/
3) https://www.globenewswire.com/news-release/2018/05/02/1494613/0/en/New-Research-Reveals-Record-Growth-in-Microservices-Is-Disrupting-the-Operational-Landscape.html

Cater to the needs of NetOps, DevOps and AppDev



NetOps

- Enables monitoring and troubleshooting for internal APIs
- Robust security ensures compliance with corporate policies



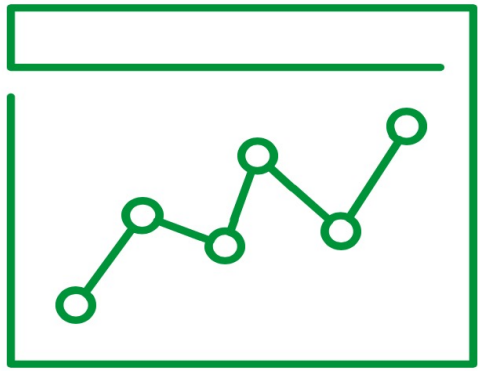
DevOps

- Drives acceleration of API release velocity by automating API management into DevOps workflows
- Self-service access frees DevOps & AppDevs to quickly create & publish APIs

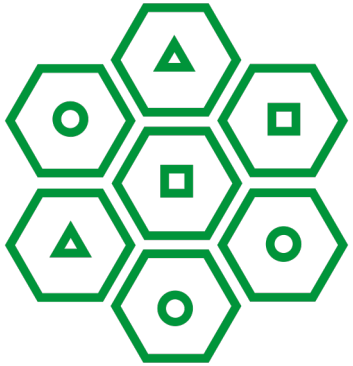
AppDev

- Proven brand – NGINX is already popular and incorporated into application stacks
- Ideal for microservices architectures and Kubernetes environment
- Easy to implement A/B, Canary, Blue/Green to test API functionality

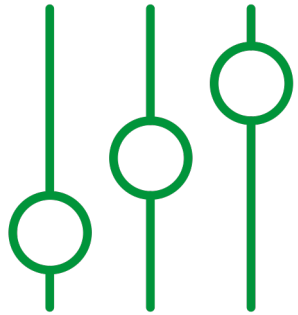
NGINX лучше всего подходит для производительности, микросервисов и DevOps



Автоматическое Управление API с интеграцией в CI / CD

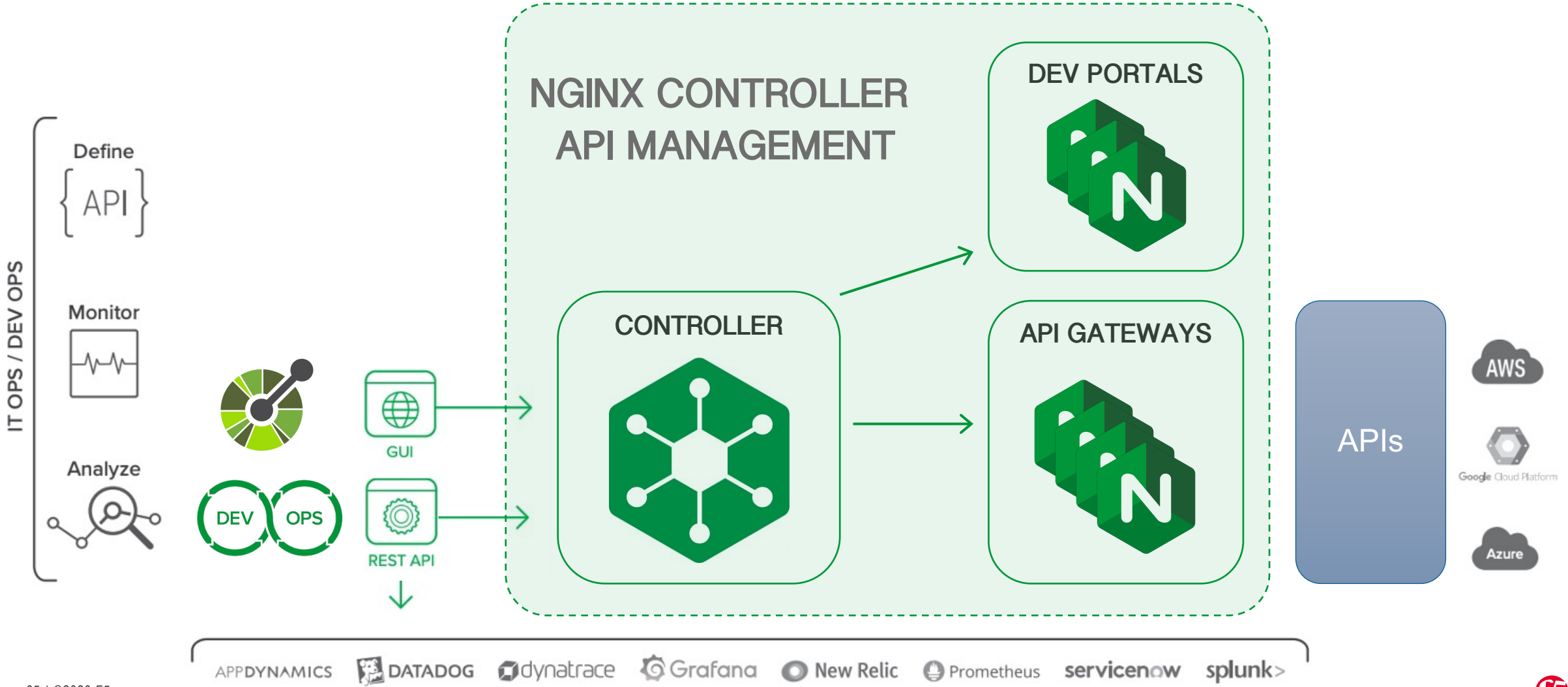


Соединение API трафика микросервисов



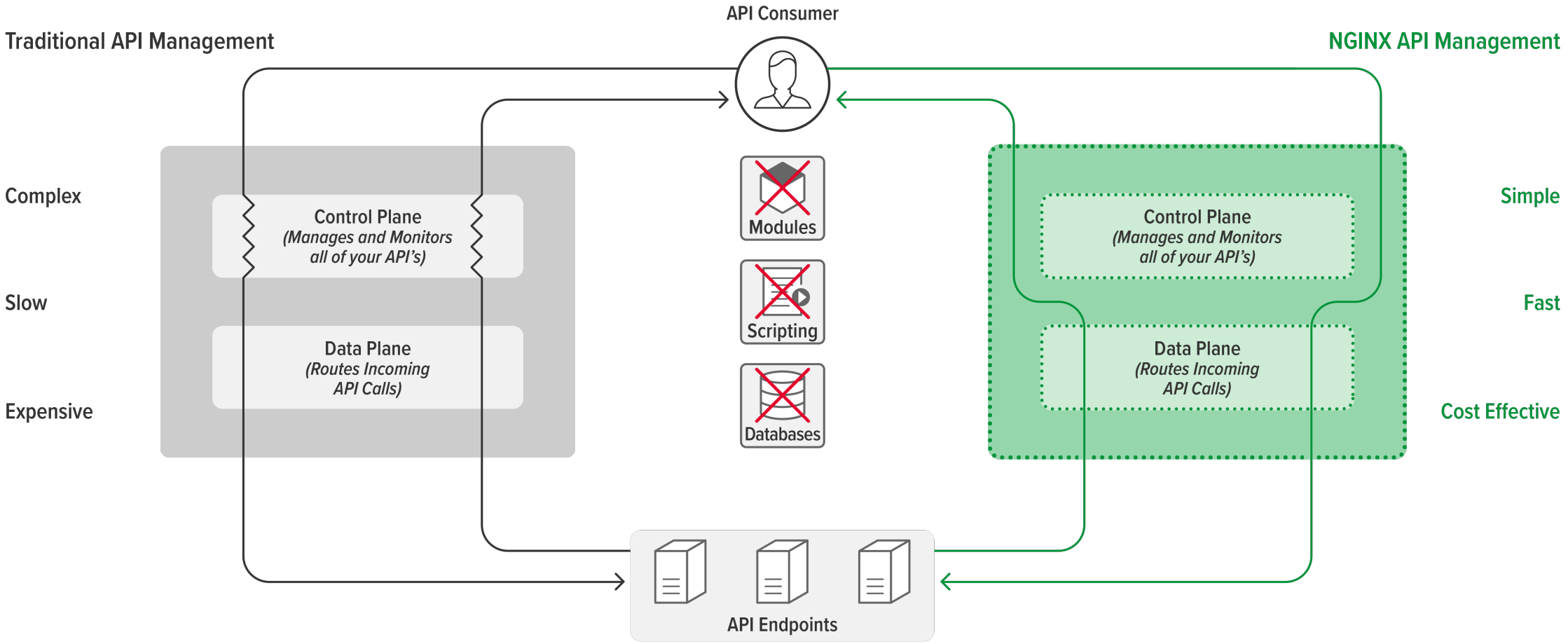
Улучшение масштаба и производительности API

NGINX управляет всем жизненным циклом API



NGINX API Management – разделенная архитектура

НЕТ ЗАВИСИМОСТИ ВРЕМЕНИ ВЫПОЛНЕНИЯ НА ШЛЮЗЕ API ОТ СИСТЕМЫ УПРАВЛЕНИЯ

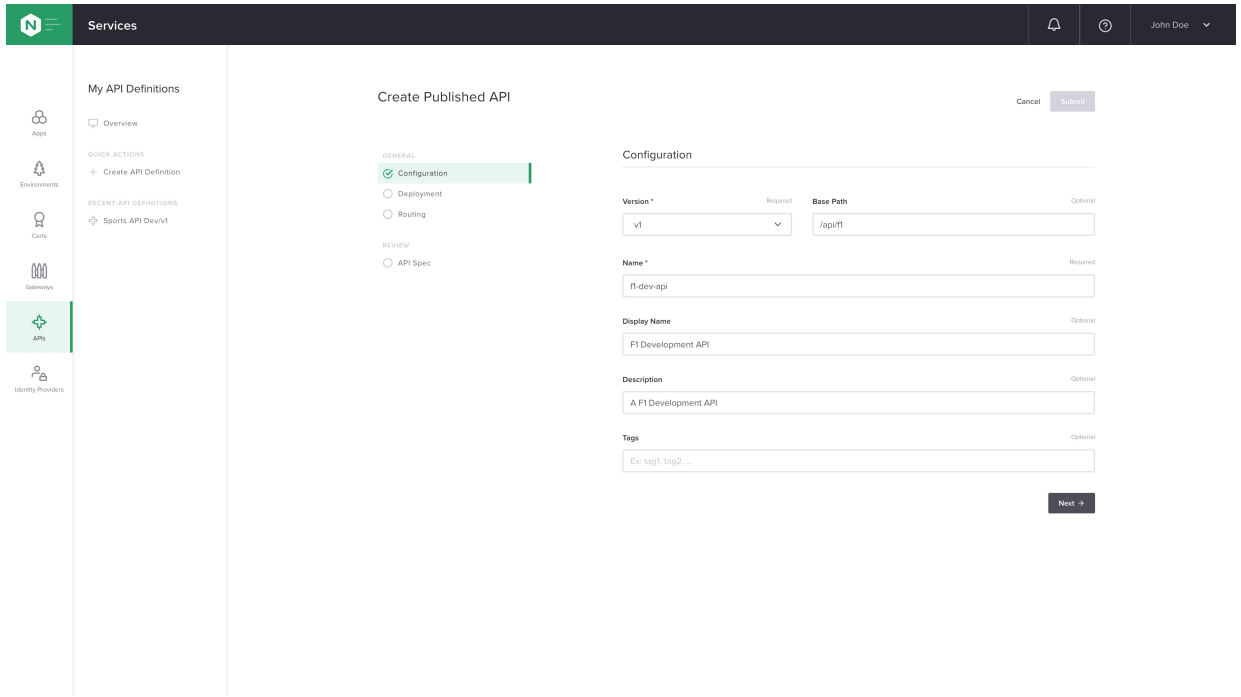


Key Capabilities

API Definition, Versioning & Publishing	Authentication & Authorization	Rate Limiting
Monitor & Analyze Performance	Dashboard	Troubleshoot Issues with Alerts
DevOps-friendly automation workflows	Export aggregated analytics data	Developer Portal

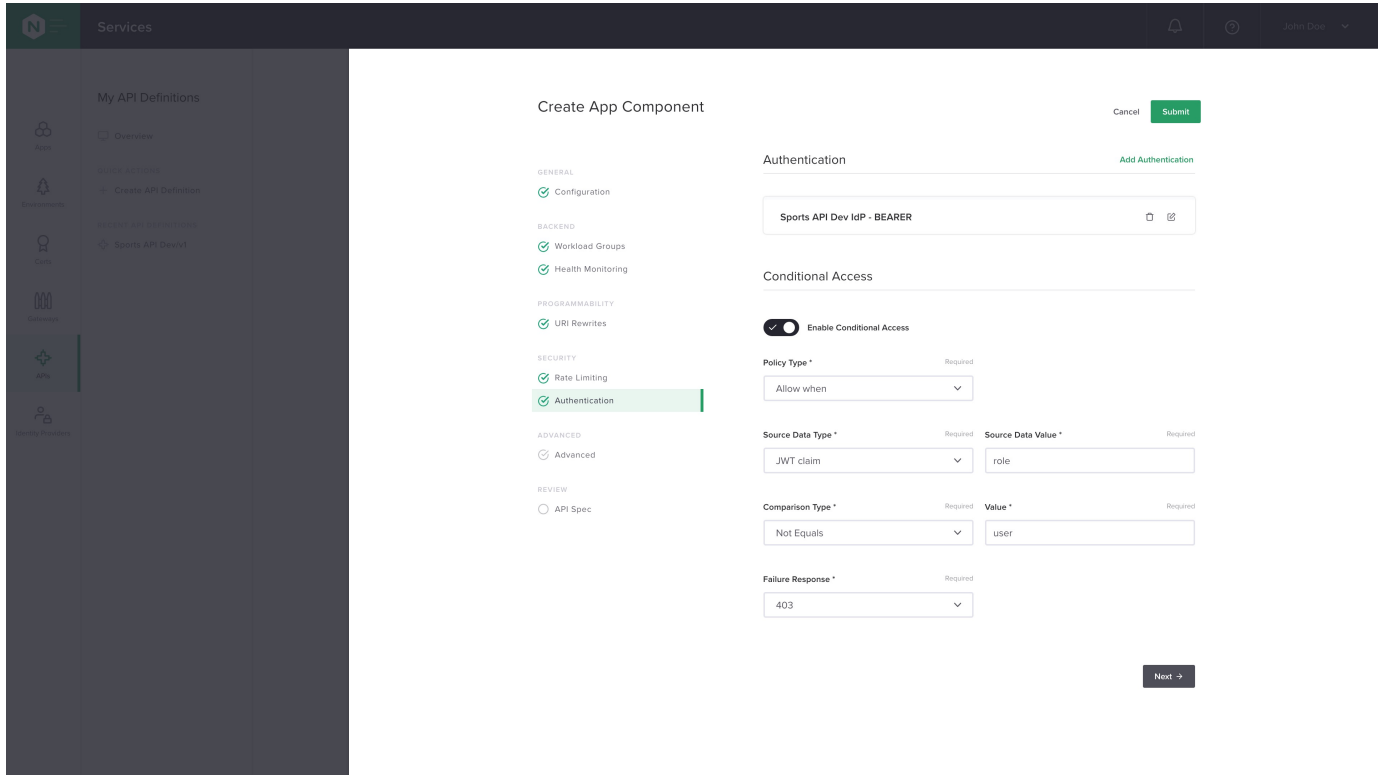
Определение и публикация API

- Create multiple API definitions using an intuitive interface
- Route resources to backend services
- Publish resulting config to NGINX Plus instances (API gateway)
- Manage versioning of APIs
- Import from Swagger/OAS
- Configure NGINX Plus as API gateway based on best practices



Аутентификация и авторизация

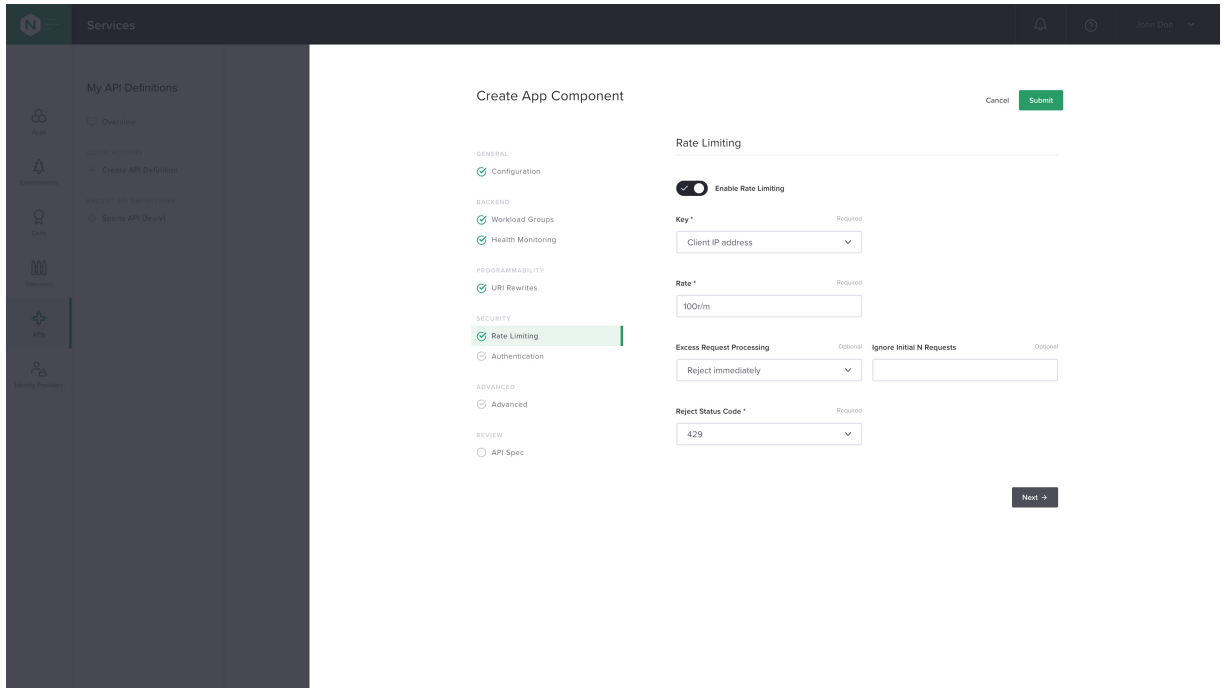
- Create and manage API keys for API consumers in order to authenticate
  and provide access to resources
- Import API keys from external systems
- Integrate with existing IdPs
- Validate JSON Web Tokens (JWTs)
- Fine-grained access control (per API endpoint) based on JWT claims



Rate Liming

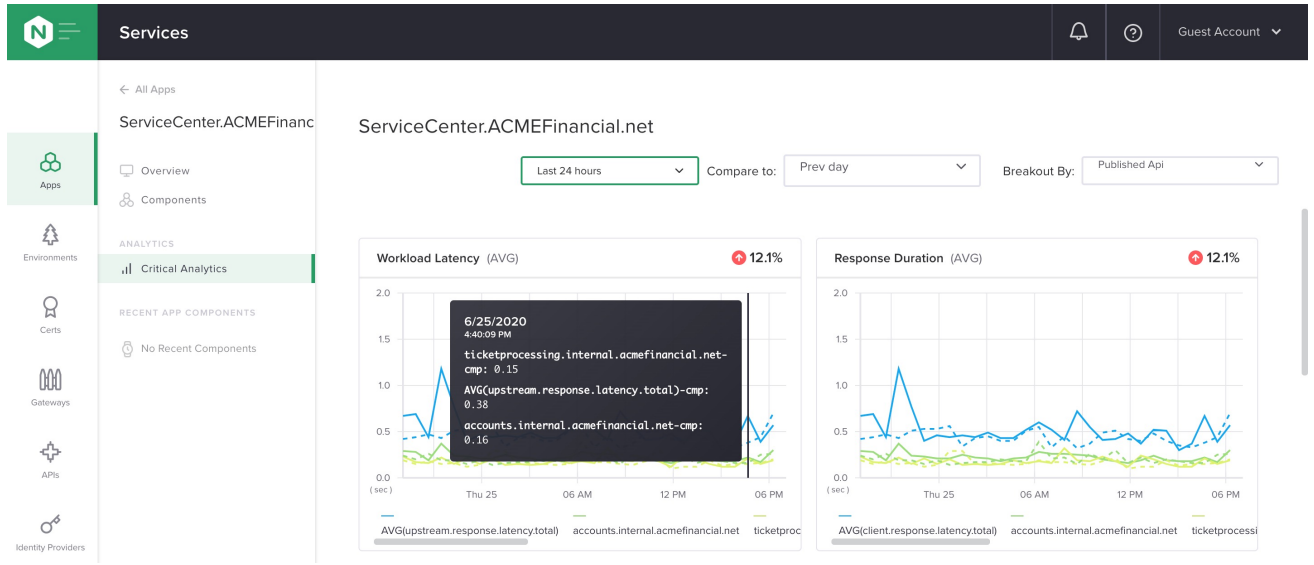
Mitigate DoS attacks and protect your applications by setting rate limits:

- Specify the maximum request rate for each client, consumer, or resource
- Enforce two-stage rate limits: delay and reject
- Protect API endpoints and ensure SLAs for API consumers
- Define multiple rate limiting policies based on the varying needs of your API consumers



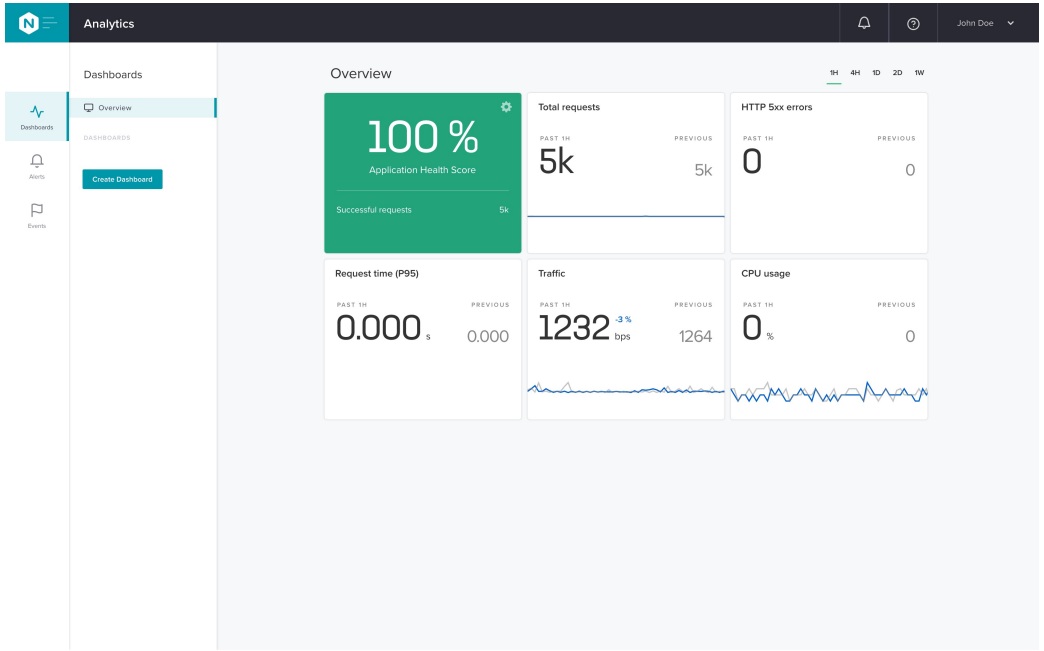
Мониторинг и анализ производительности

- Gain deep visibility and insights into KPIs such as latency and response time on a per API basis
- Troubleshoot performance issues faster
- Analyze usage and performance trends for 200 metrics from the OS to individual NGINX Plus instances (API GWs)



Dashboarding

- Get a summary view including CPU usage, performance, and errors across multiple gateways
- Measure successful requests and timely responses on aggregate
- Verify environment health and showcase to key stakeholders
- Customize dashboards—from scratch or from pre-defined templates—and measure what matters to you



Real-time alerting

- Meet application performance and reliability SLAs
- Keep your finger on the pulse of your APIs with threshold trigger alerting
- Reduce troubleshooting time and effort with accurate, specific, real-time error alerts

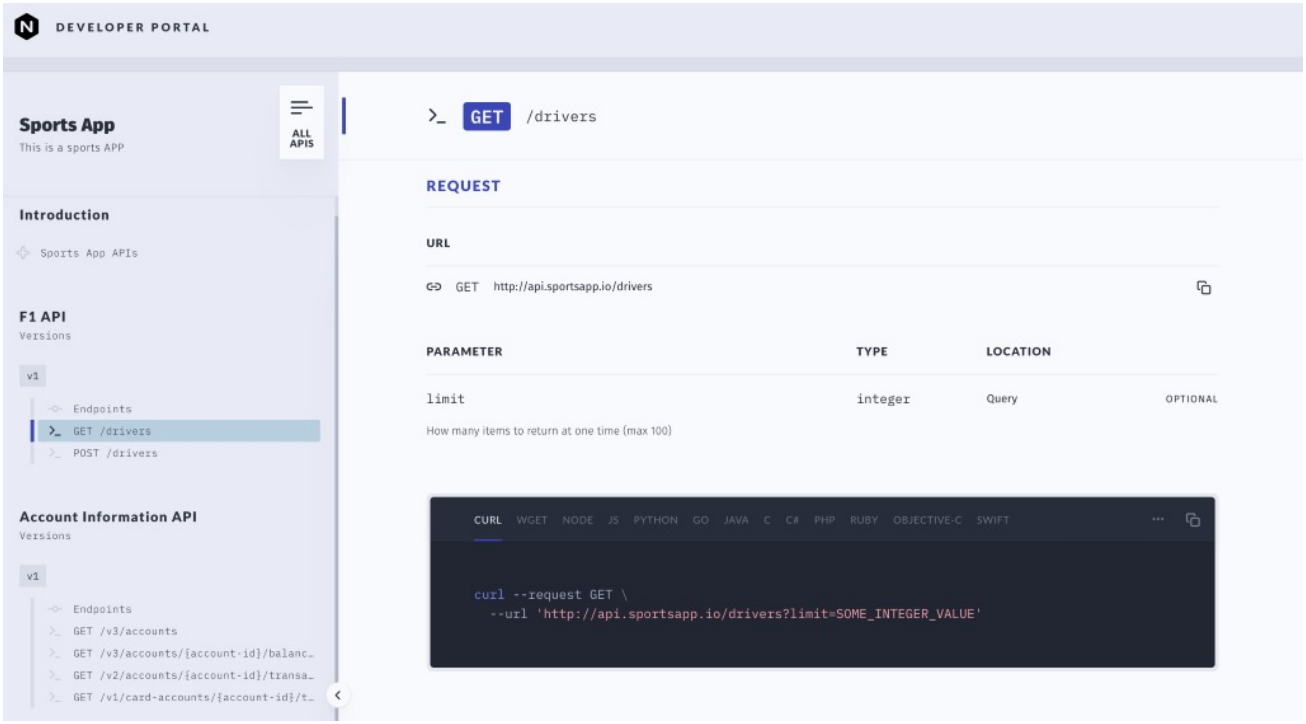
Возможности для DevOps

Accelerate API release velocity

- Integrate API management into DevOps workflows and CI/CD pipelines using APIs
- Define and publish APIs
- Configure API gateways
- Configure security policies for published APIs
- Deploy and run on containers

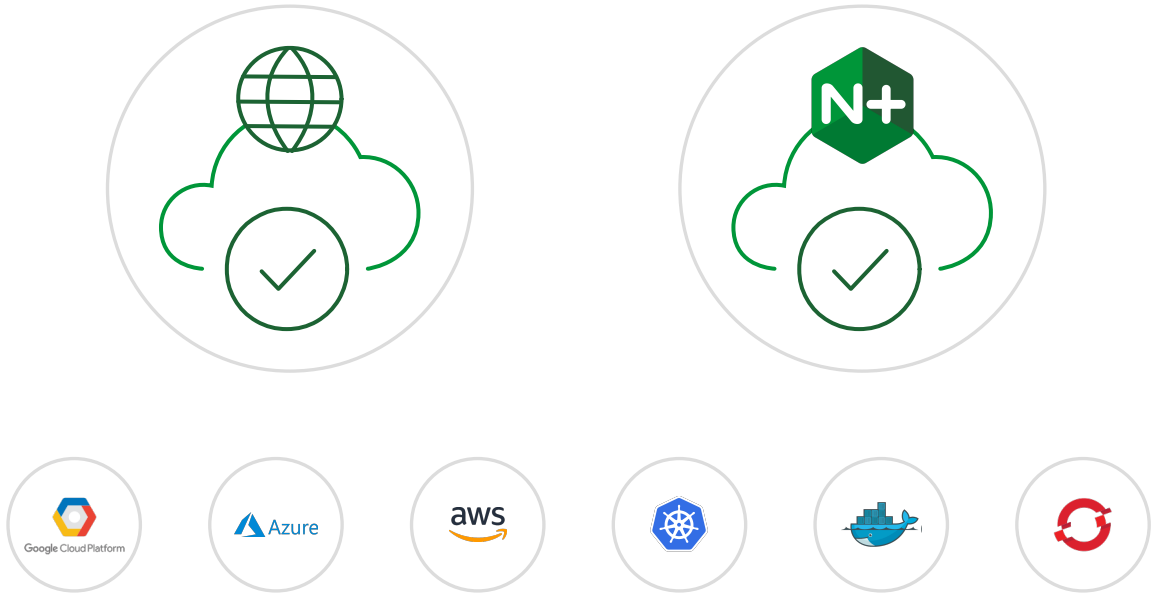
Портал разработчика

- Host developer portal on a logically separate NGINX web server for added performance and availability.
- Flexible deployment options – separate environment to API gateways
- Deploy multiple portals (internal vs external, branding)
- Quickly generate the following for efficient onboarding by developers who consumer your APIs
  - Catalog of all published APIs
  - Documentation
  - Code samples



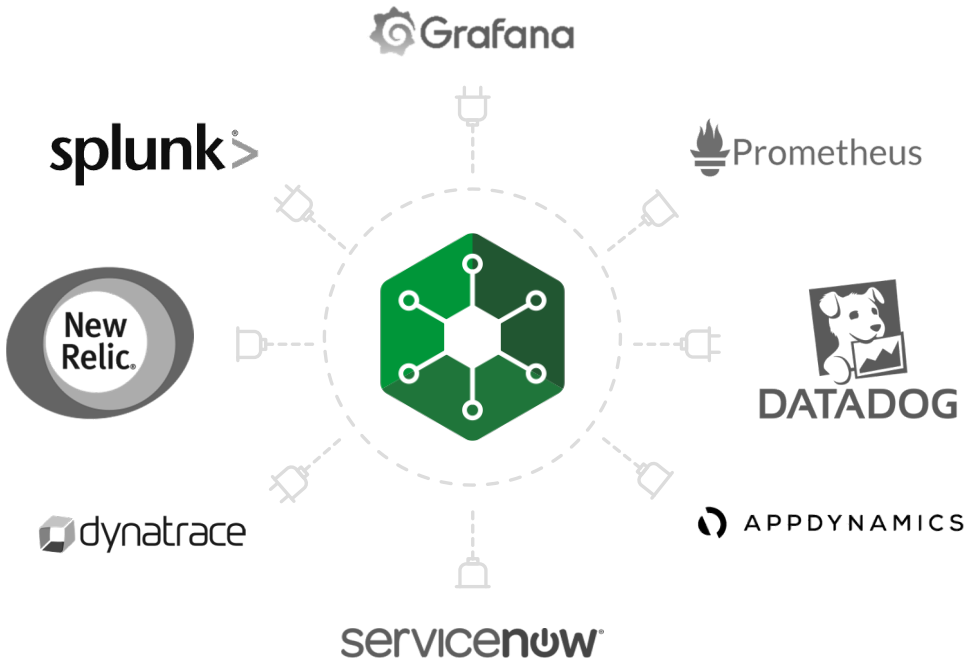
Поддержка различных сред в одной системе

- Support every application and API, in any cloud
- Gain deployment flexibility—NGINX Controller is a Docker package, deployable anywhere
- Spin up Controller and API GWs (NGINX Plus instances) on any public or private cloud
- Manage NGINX Plus instances on any public or private cloud



Сторонние интеграции

- Securely extract meaningful health and performance metrics
- Integrate into monitoring tool of choice
- Get the most out of your existing monitoring and analytics software investments
- Leverage fast, reliable REST APIs



NGINX App Protect

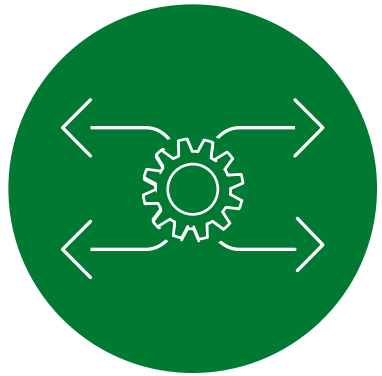
Сегодня мы строит ИТ сервисы по новому

Конфиденциа-льные данные

Половина приложений остается уязвимой.

Мульти-среды

Преобразование создает проблемы для эксплуатации и безопасности.



API

API-интерфейсы эксплуатируются и ими злоупотребляют.

Уязвимости ПО и распространенные векторы атак

УЯЗВИМОСТИ В КОМПОНЕНТАХ ИНФРАСТРУКТУРЫ (CVEs)

Программные уязвимости обнаруживаются в компонентах практически всех программных стеков.

- Operating systems (Windows, Linux, containers)
- Application servers
- Support libraries
- Programming languages
- 3rd party libraries (NPM, CPAN, Ruby Gems)

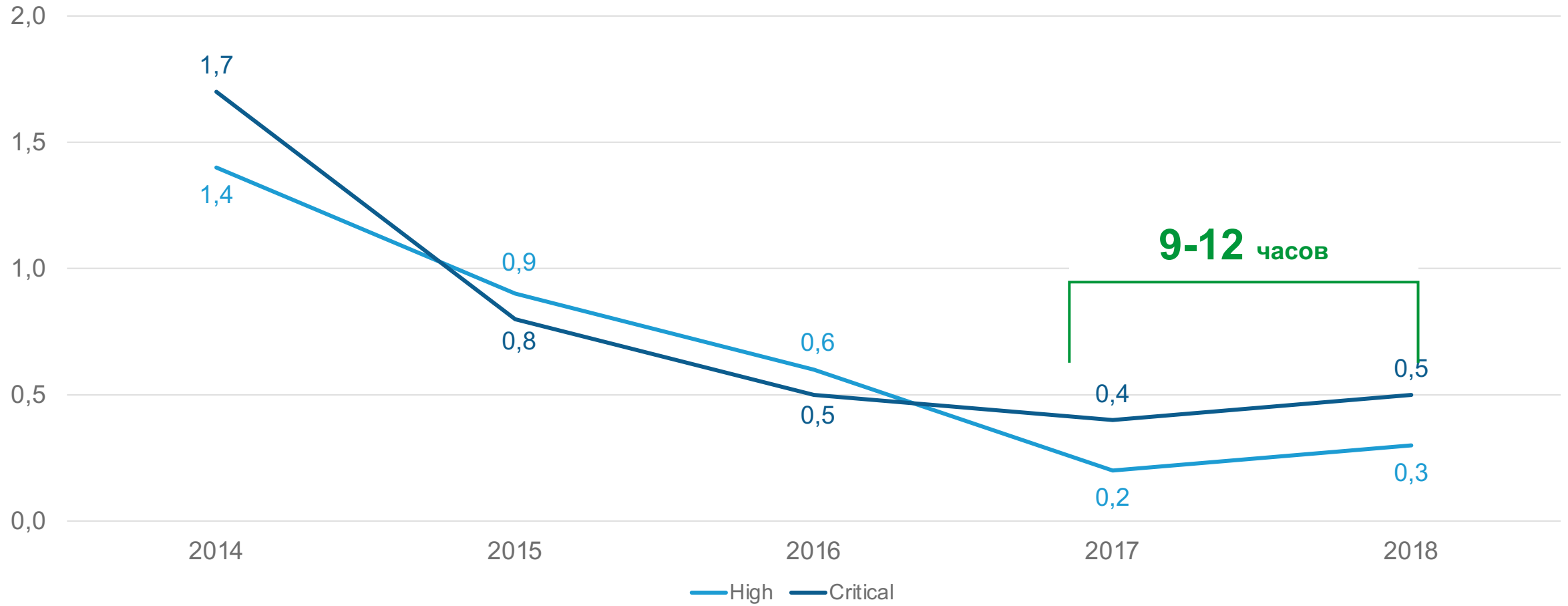
ЧАСТОЯ ПОЯВЛЯЮЩИЕСЯ ПРОБЛЕМЫ В КОДЕ ПРИЛОЖЕНИЯ (OWASP Top 10)

Такие угрозы, как Injection и XSS, хорошо известны, но их трудно устранить, поэтому они широко распространены.

- Injection
- Cross Site Scripting
- Cross-site request forgery
- Insecure deserialization

Уязвимости выявляются быстрее, чем организации могут их исправить

СРЕДНЕЕ КОЛИЧЕСТВО ДНЕЙ МЕЖДУ ВЫПУЩЕННЫМИ "ВЫСОКИМИ" И "КРИТИЧЕСКИМИ" CVE



РЕАЛЬНОСТЬ: ДИСБАЛАНС ЭДЖАЙЛ

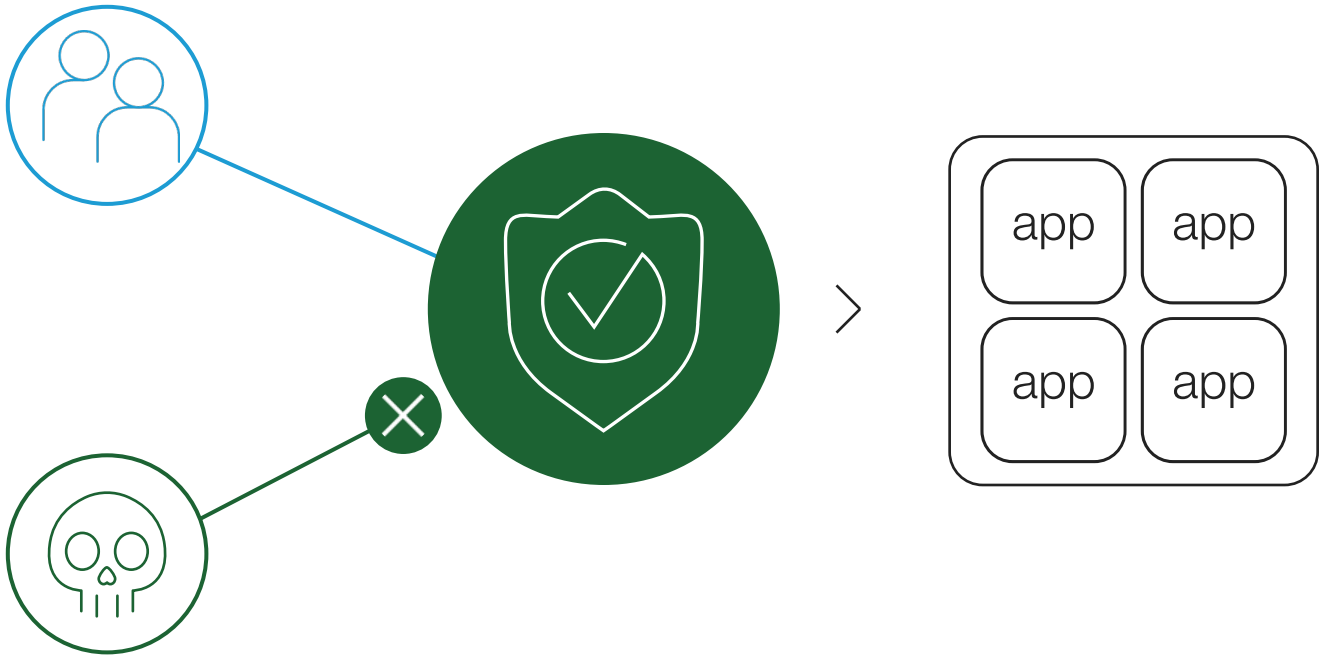
100	10	**1**
Разработчики	DevOps	**Безопасность**

Конвейер создан для скорости, а не для безопасности

Последовательные политики безопасности часто не подходят для гибких и облачных сред.

Цели контроля безопасности не могут быть адекватно применены и обеспечены

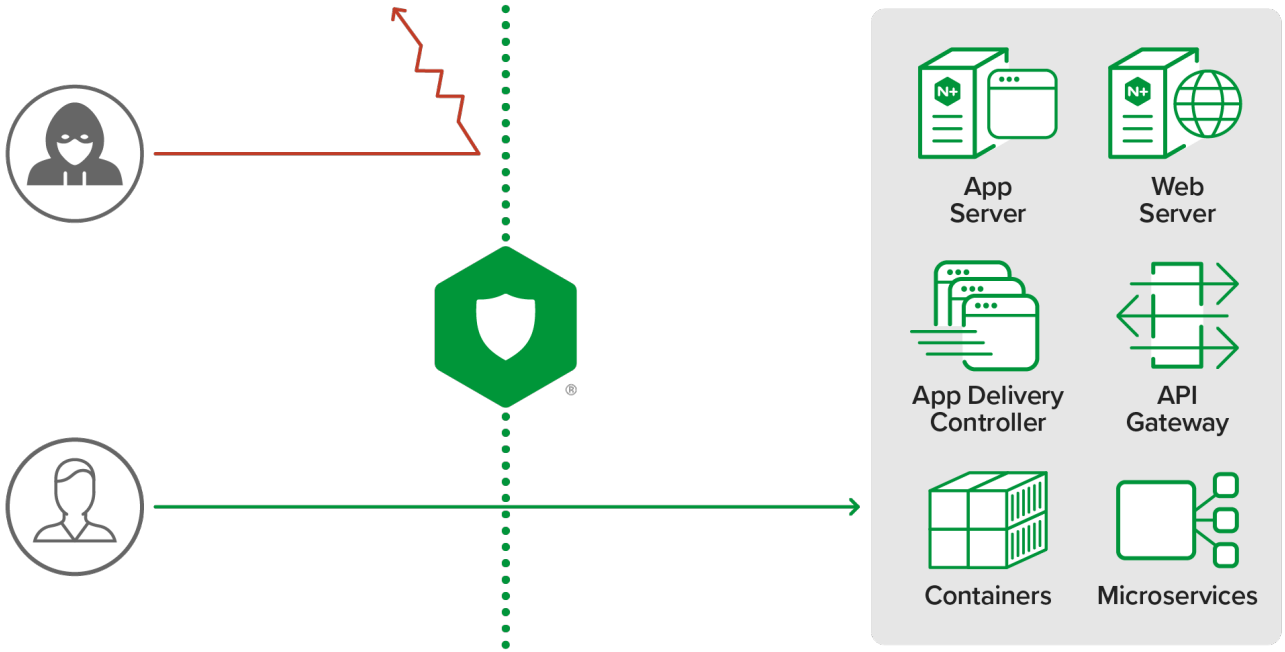
How do you protect apps?



- Vulnerabilities
- Active attacks
- Risk and address compliance

NGINX App Protect

ЗАЧЕМ ПЕРЕХОДИТЬ НА ЗАЩИТУ ПРИЛОЖЕНИЯ ОТ NGINX



Secure

- Высокая производительность
- Защита не только на основе сигнатур
- Надежные сигнатуры от F5

CI/CD Friendly

- Простая интеграция CI / CD
- Разработан для современной инфраструктуры
- Быстрая обратная связь для правок политики

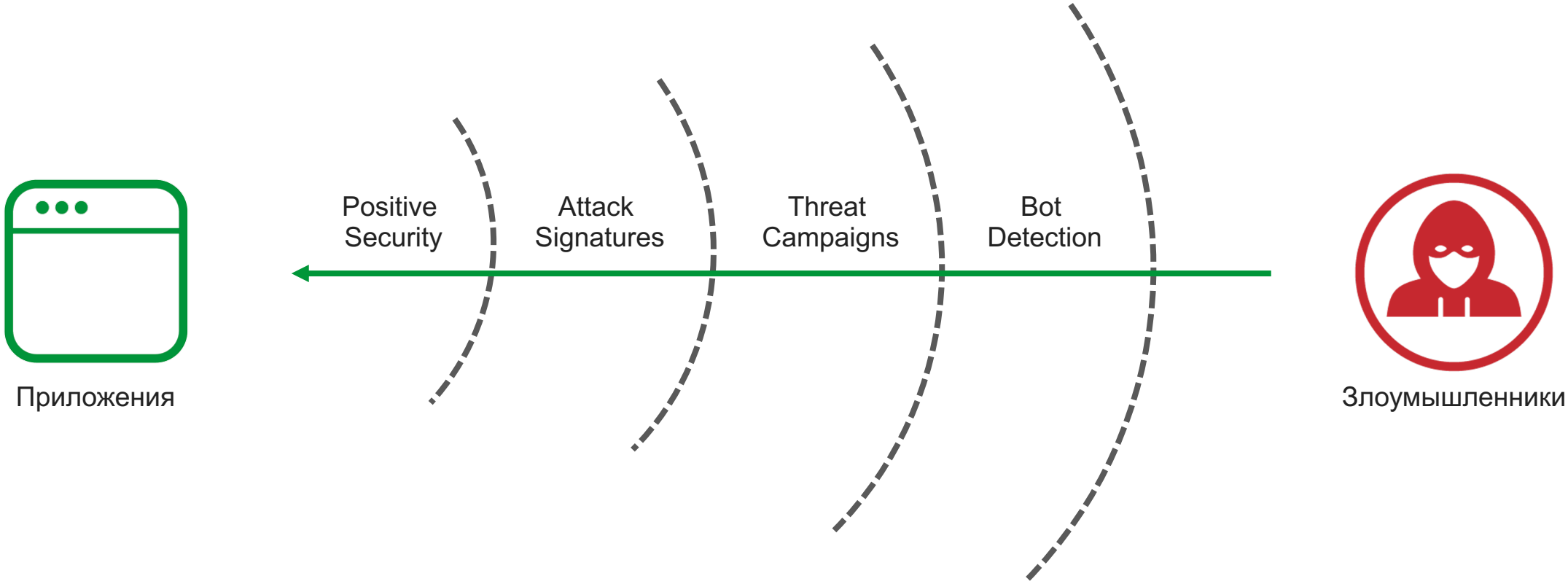
Manage

- Единый декларативный интерфейс F5
- Статистика безопасности syslog
- Поддерживается через F5 Support

NGINX Part of F5

NGINX App Protect - Надежная безопасность приложений

A MULTILAYER APPROACH



NGINX Part of F5

NGINX App Protect – Bot Protection

СНАЧАЛА БЛОКИРУЙТЕ АВТОМАТИЗИРОВАННЫЕ АТАКИ

- Сигнатуры ботов обеспечивают базовую защиту ботов, обнаруживая сигнатуры ботов в заголовке User-Agent и URI.
- Каждая сигнатрура бота определяет его класс
  - Trusted Bot
  - Untrusted Bot
  - Malicious Bot

- **Огромное количество планов развития**

```
{
    "policy": {
        "name": "bot_defense_policy",
        "template": {
            "name": "POLICY_TEMPLATE_NGINX_BASE"
        },
        "applicationLanguage": "utf-8",
        "enforcementMode": "blocking",
        "bot-defense": {
            "settings": {
                "isEnabled": true
            },
            "mitigations": {
                "classes": [
                    {
                        "name": "trusted-bot",
                        "action": "alarm"
                    },
                    {
                        "name": "untrusted-bot",
                        "action": "block"
                    },
                    {
                        "name": "malicious-bot",
                        "action": "block"
                    }
                ]
            }
        }
    }
}
```

NGINX App Protect – Threat Campaign

ЗАЩИТИТЕ ВАШЕ ПРИЛОЖЕНИЕ ОТ ТЕКУЩИХ АТАК

- Threat Campaigns - это функция анализа угроз.
- Частые обновления, содержащие информацию об активных атаках.
- Контекстная информация Threat Campaigns очень специфична для текущих атакующих кампаний.
- Ложных срабатываний практически не существует.

Пример :

APT12 are exploiting Apache Struts2 (CVE-2018-11776) to deploy crypto-miner

NGINX App Protect – Политика по умолчанию

ПОСЛЕДОВАТЕЛЬНАЯ ПОЛИТИКА ПО УМОЛЧАНИЮ

- OWASP Top 10 based attack signatures & CVEs
- Evasion techniques

Негативная безопасность

- Meta characters check
- HTTP protocol compliance
- Disallowed file types (bin, cgi, cmd, com, dll, exe, msi, sys, shtm, shtml, stm & more)
- Cookie integrity check
- JSON & XML well-formedness
- Sensitive parameters & Data Guard

Позитивная безопасность

NGINX App Protect – Attack Signatures

ADAPT SIGNATURES APPLIED TO YOUR APPLICATION

Apply different Basic Signature Sets :

- All Response Signatures
- All Signatures
- Generic Detection Signatures
- Generic Detection Signatures (High Accuracy)
- Generic Detection Signatures (High/Medium Accuracy)
- High Accuracy Signatures
- Low Accuracy Signatures
- Medium Accuracy Signatures
- OWA Signatures
- WebSphere signatures

Or customize your App Protect policy with more than 80 Server Technology :

Sharepoint, Python, Vue.JS, GraphQL, NodeJS, Angular, React, Express.JS, Wordpress, Linux, XML, PHP, Windows …

NGINX App Protect – Positive Model

PROTECT APPLICATION ABOUT POTENTIAL 0-DAYS ATTACKS

Use the positive model to tighten the security policy using :

- **Dataguard** – protect your sensitive data in response
- **File types** – enable/disable specific file types
- **HTTP Methods** - what methods to allow or disallow.
- **HTTP Response Codes** – response codes allowed
- **HTTP Parameters** – detect and control parameters
- **HTTP URL** - what URL to allow or disallow
- **Content Profile –** JSON / XML …

… Or use them to make specific exceptions !

```
{
    "entity": {
        "name": "/vulnerabilities/sqli*"
    },
    "entityChanges": {
        "signatureOverrides": [
            {
                "signatureId": 200002147,
                "enabled": false
            },
            {
                "signatureId": 200002835,
                "enabled": false
            },
            {
                "signatureId": 200002476,
                "enabled": false
            }
        ]
    },
    "entityType": "url",
    "action": "add-or-update"
}
```

NGINX App Protect – Позитивная безопасность

ЗАЩИЩАЙТЕ API С ПОМОЩЬЮ ФАЙЛА OPENAPI ИЛИ СХЕМЫ JSON

```
{
    "policy": {
        "name": "json_form_policy_external_schema",
        "template": {
            "name": "POLICY_TEMPLATE_NGINX_BASE"
        },
        "json-validation-files": [
            {
                "fileName": "person_schema.json",
                "link": "file://person_schema.json"
            }
        ],
        "json-profiles": [
            {
                "name": "reg_form_prof",
                "defenseAttributes": {
                    "maximumArrayLength": "any",
                    "maximumStructureDepth": "any",
                    "maximumTotalLengthOfJSONData": 10
                    "maximumValueLength": "any",
                    "tolerateJSONParsingWarnings": fal
                },
                "validationFiles": [
                    {
                        "isPrimary": true,
                        "jsonValidationFile": {
                            "fileName": "person_schema.json"
                        }
```

```
{
    "policy": {
        "name": "petstore_api_security_policy",
        "description": "NGINX App Protect API Security Policy for the Petstore API",
        "template": {
            "name": "POLICY_TEMPLATE_NGINX_BASE"
        },
        "open-api-files": [
            {
                "link": "http://127.0.0.1:8088/myapi.yaml"
            }
        ],
        "violations": [
            {
                "block": true,
                "description": "Disallowed file upload content detected in body",
                "name": "VIOL_FILE_UPLOAD_IN_BODY"
            },
            {
```


NGINX Part of F5

NGINX App Protect – Ложноположительные сигналы

ОПРЕДЕЛИТЕ ЛОЖНЫЕ СРАБАТЫВАНИЯ И СПРАВЬТЕСЬ С НИМИ

Рейтинг нарушений определяется для каждого запроса и помогает администратору квалифицировать ложное срабатывание.

Используйте **Attack Signature False Positive Mode (by default)** для блокировки на основе рейтинга нарушения.

method	uri	violations	violation_rating	request_status
GET	/login.php	HTTP protocol compliance failed	3	alerted
GET	/manager/html	HTTP protocol compliance failed, Bot Client Detected	3	alerted
GET	/wp-login.php	HTTP protocol compliance failed, Bot Client Detected	3	alerted
POST	/_ignition/execute-solution	HTTP protocol compliance failed, Illegal meta character in value	2	alerted
POST	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php	HTTP protocol compliance failed, Illegal meta character in value, Illegal meta character in parameter name, Attack signature detected, Violation Rating Threat detected	4	blocked
GET	/	HTTP protocol compliance failed	3	alerted

0	No Violation
1	False Positive
2	False Positive
3	Needs Examination
4	Threat
5	Threat

NGINX Part of F5

NGINX App Protect – Мониторинг

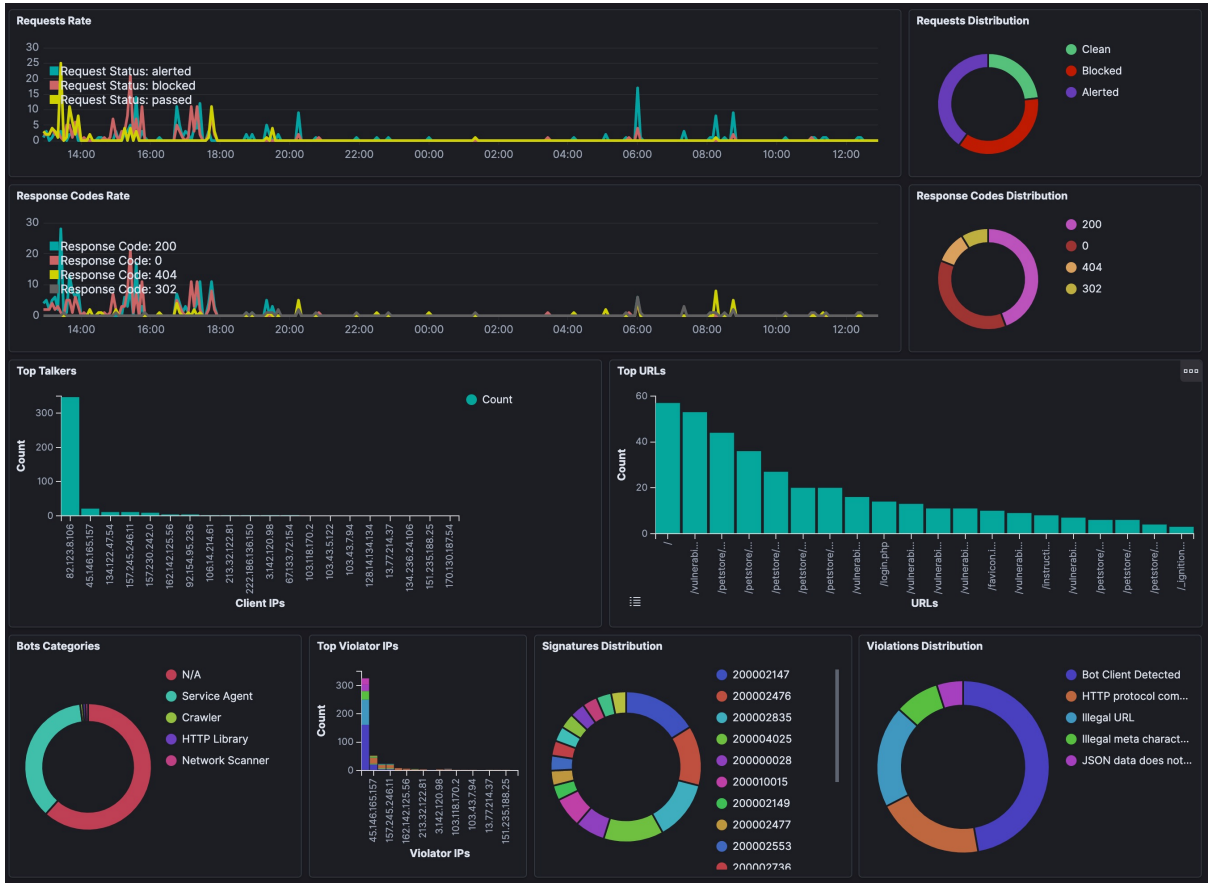
ПОЛУЧАЙТЕ ПОЛНУЮ ИНФОРМАЦИЮ О ТРАФИКЕ, НАРУШЕНИЯХ И МЕРАХ ПО ИХ УСТРАНЕНИЮ

Журнал безопасности содержит:

- Информация о HTTP запросах и ответах
- Как NGINX App Protect поступает с траификом
- Блокировка на основе настроенных параметров политики

… экспорт логов через stderr, файл или syslog:

```
app_protect_security_log "/etc/app_protect/conf/log_default.json" syslog:server=localhost:5144;
app_protect_security_log "/etc/app_protect/conf/log_default.json" /var/log/app_protect/security.log;
app_protect_security_log "/etc/app_protect/conf/log_default.json" stderr;
```



Панель управления ELK доступна на:

https://github.com/f5devcentral/f5-waf-elk-dashboards

NGINX Part of F5

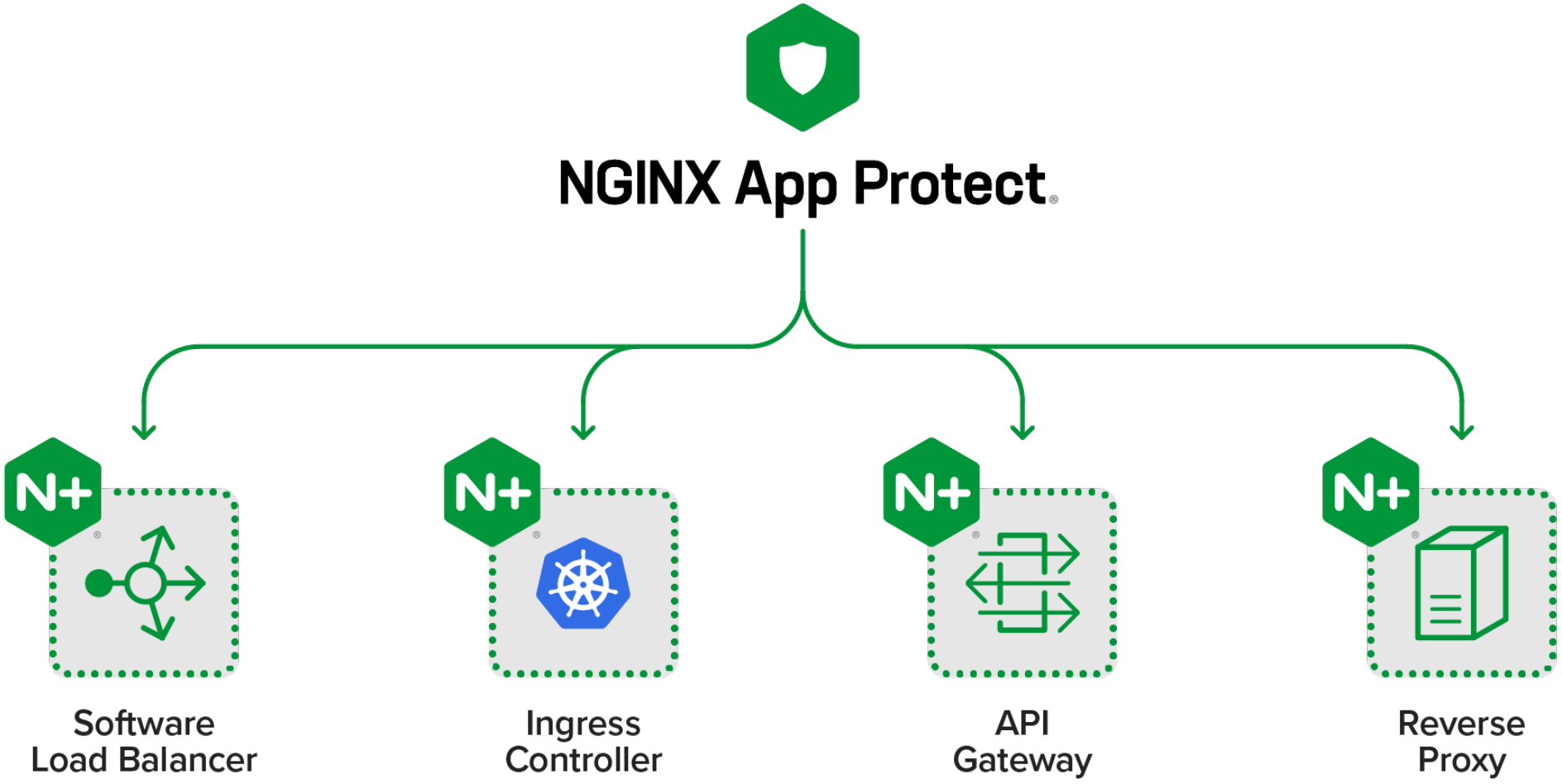
NGINX App Protect для современных приложений

ВСТРОЕННАЯ ИНТЕГРАЦИЯ В NGINX

```
http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;

    app_protect_enable on; # This is how you enable NGINX App Protect in the relevant context/bloc
    app_protect_policy_file "/etc/nginx/NginxDefaultPolicy.json"; # This is a reference to the pol
    app_protect_security_log_enable on; # This section enables the logging capability
    app_protect_security_log "/etc/app_protect/conf/log_default.json" syslog:server=127.0.0.1:515;

    server {
        listen       80;
        server_name  localhost;
        proxy_http_version 1.1;

        location / {
            client_max_body_size 0;
            default_type text/html;
            proxy_pass http://172.29.38.211:80$request_uri;
        }
    }
```

NGINX App Protect для современных приложений

ВАРИАНТЫ РАЗВЕРТЫВАНИЯ



NGINX App Protect – совместим с CI/CD

ДЕКЛАРАТИВНАЯ ПОЛИТИКА

1. Support Base Templates

```
http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;

    app_protect_enable on; # This is how you enable NGINX App Prote
    app_protect_policy_file "/etc/nginx/NginxDefaultPolicy.json";
    app_protect_security_log_enable on; # This section enables the
    app_protect_security_log "/etc/app_protect/conf/log_default.jso

    server {
        listen       80;
        server_name  localhost;
        proxy_http_version 1.1;

        location / {
            client_max_body_size 0;
            default_type text/html;
            proxy_pass http://172.29.38.211:80$request_uri;
        }
    }
```

ики

политиками.

```
{
    "policy": {
        "name": "signature_modification_entitytype",
        "template": { "name": "POLICY_TEMPLATE_NGINX_BASE" },
        "applicationLanguage": "utf-8",
        "enforcementMode": "blocking",
        "signature-sets": [
            {
                "name": "All Signatures",
                "block": true,
                "alarm": true
            }
        ]
    },
    "modifications": [
        {
            "entityChanges": {
                "enabled": false
            },
            "entity": {
                "signatureId": 200001834
            },
            "entityType": "signature",
            "action": "add-or-update"
        }
    ]
}
```

NGINX App Protect – CI/CD

ДЕКЛАРАТИВНАЯ ПОЛИТИКА - ВНЕШНЯЯ ССЫЛКА

Из файловой системы или HTTP(s) WebServer/Repository

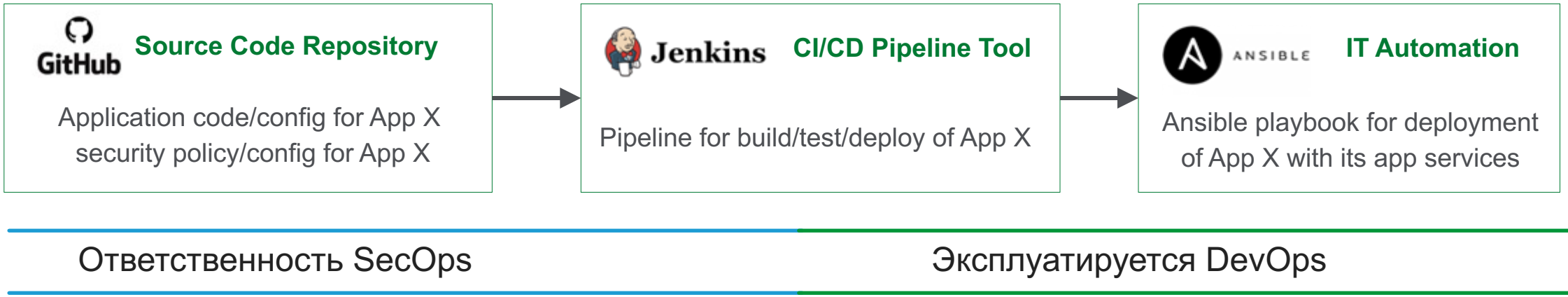
```
{
    "name": "external_resources_file_types",
    "template": {
        "name": "POLICY_TEMPLATE_NGINX_BASE"
    },
    "applicationLanguage": "utf-8",
    "enforcementMode": "blocking",
    "blocking-settings": {
        "violations": [
            {
                "name": "VIOL_FILETYPE",
                "alarm": true,
                "block": true
            }
        ]
    },
    "filetypeReference": {
        "link": "http://domain.com:8081/file-types.txt"
    }
}
```


```
[
    {
        "name": "*",
        "type": "wildcard",
        "allowed": true,
        "checkPostDataLength": false,
        "postDataLength": 4096,
        "checkRequestLength": false,
        "requestLength": 8192,
        "checkUrlLength": true,
        "urlLength": 2048,
        "checkQueryStringLength": true,
        "queryStringLength": 2048,
        "responseCheck": false
    },
    {
        "name": "pat",
        "allowed": false
    },
    {
        "name": "mat",
        "allowed": false
    }
]
```


NGINX Part of F5

NGINX App Protect – работа с CI/CD

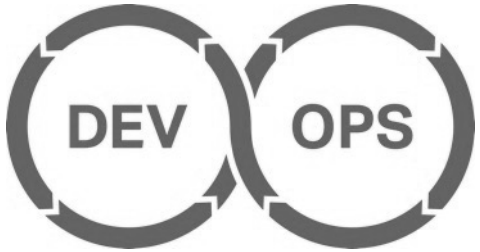
DEVSECOPS И БЕЗОПАСНОСТЬ КАК КОД




```
{
  "entityChanges": {
    "type": "explicit"
  },
  "entity": {
    "name": "bak"
  },
  "entityKind":
"tm:asm:policies:filetypes:filetypestate",
  "action": "delete",
  "description": "Delete Disallowed File Type"
}
```

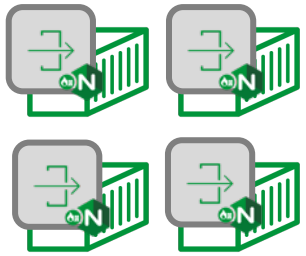
NGINX App Protect – CI/CD Friendly

KEY USE CASE



Embed Security Policy Your Pipeline

Integrate security controls directly into your pipeline with security as code.



Secure Modern Apps

Strong security controls for microservices, containers, APIs, and other modern topologies.

Improve App Performance

The high performance WAF drives down operational costs and improve user the user experience without compromising security.

F5 NGINX App Protect

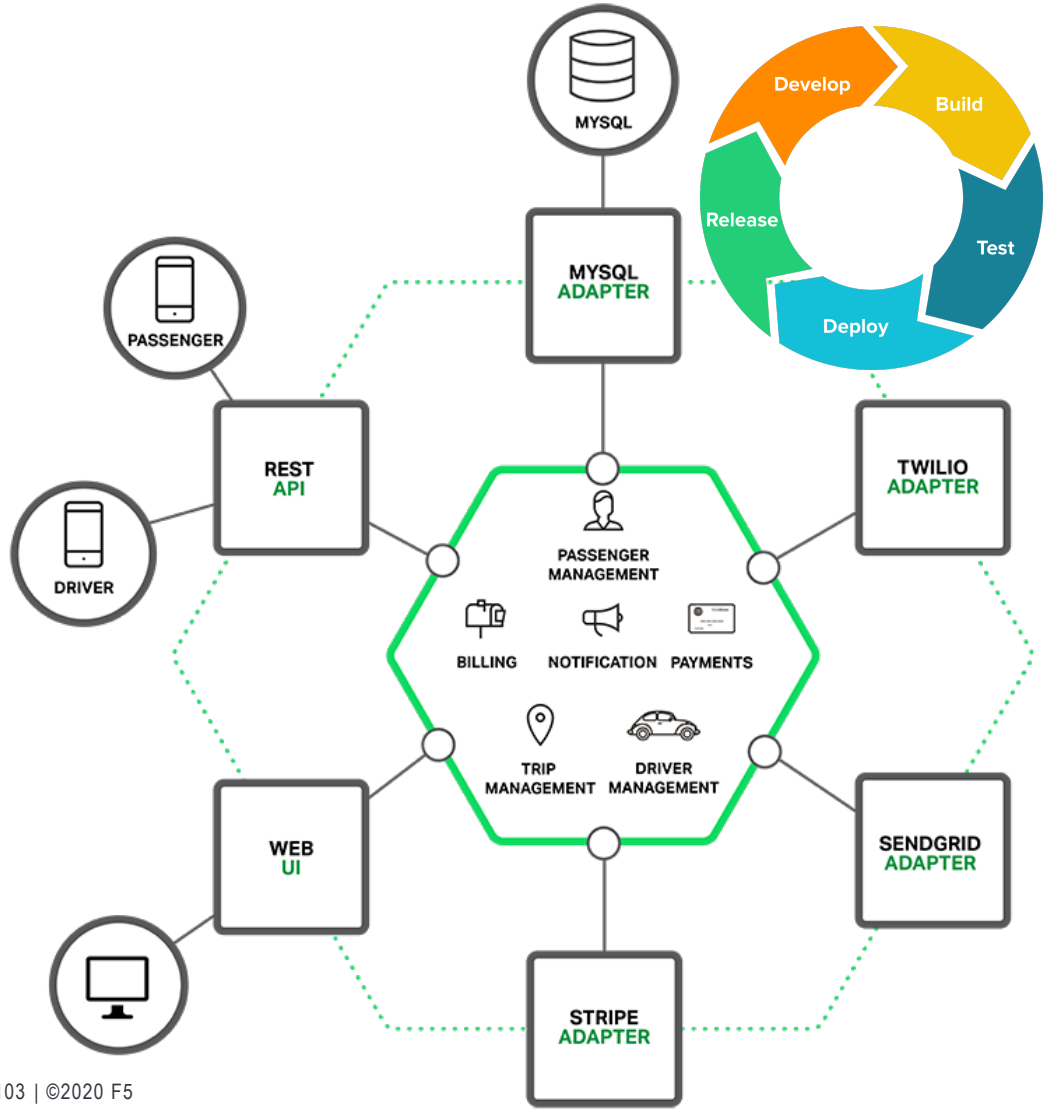
Надежная безопасность для ваших приложений

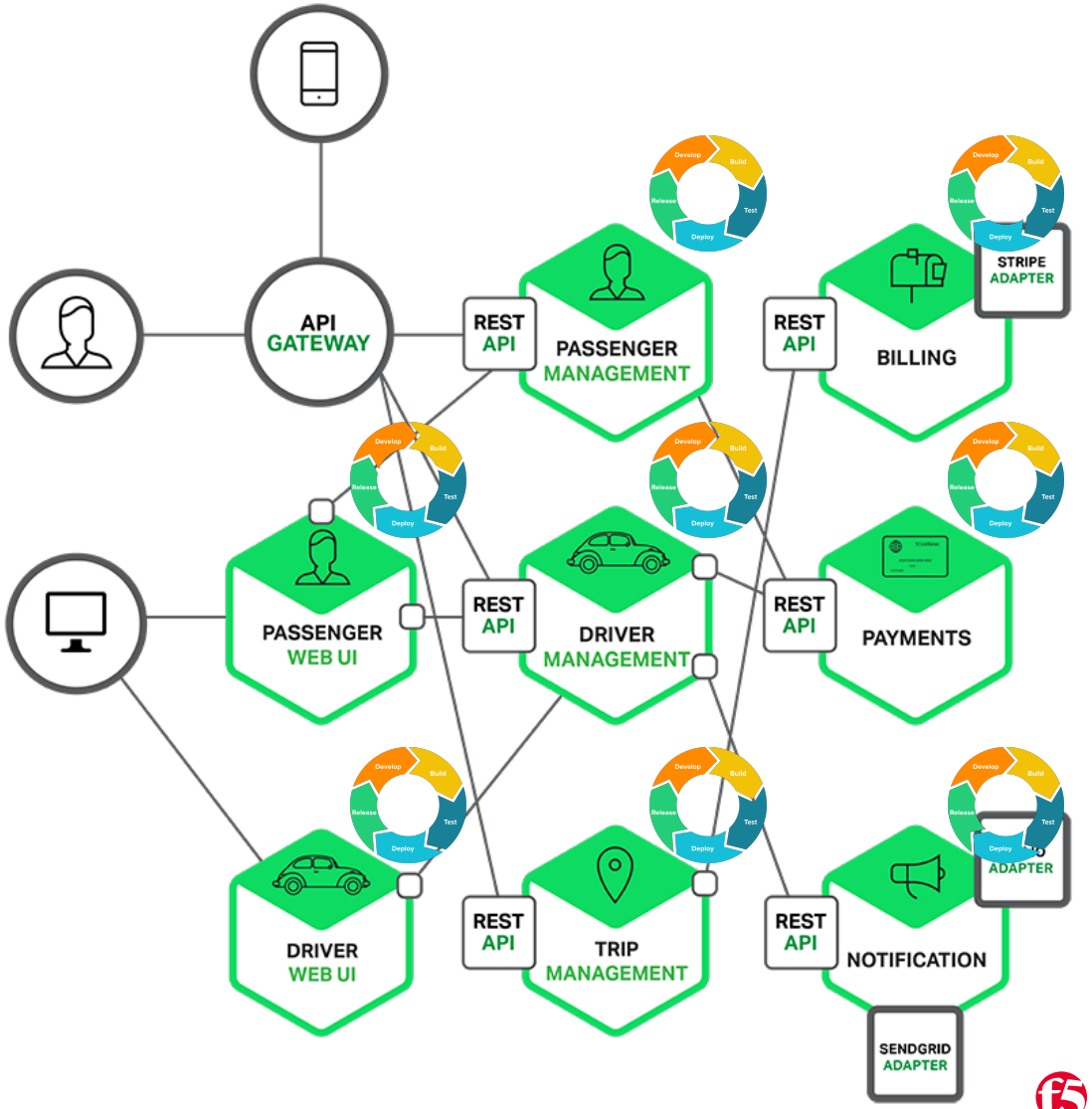
Создан для современных приложений

Совместимость с CI / CD

Microservices

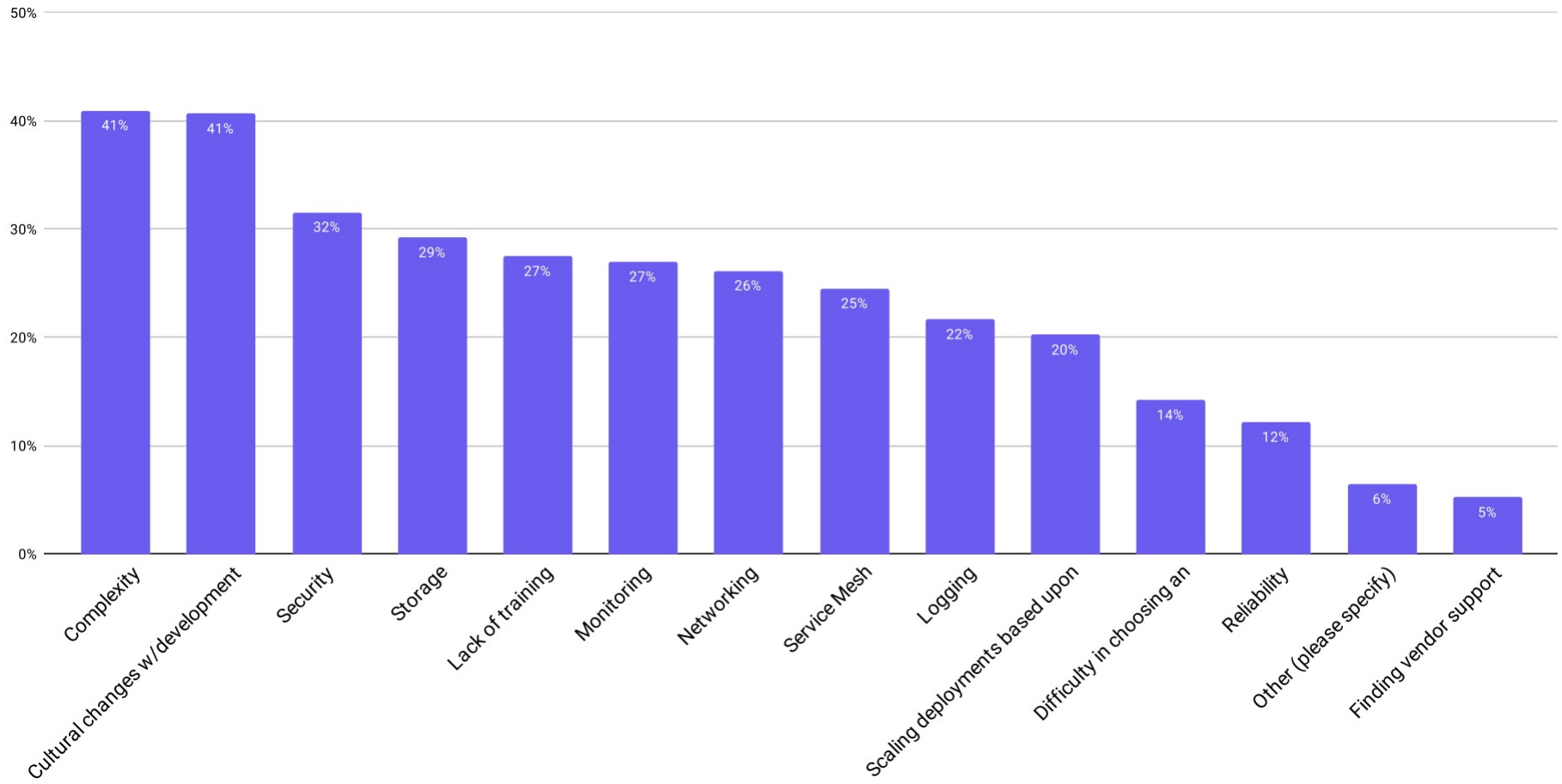
Как выглядит ваша прикладная артитектура?





Проблемы при внедрении контейнеров

ИСТОЧНИК: CNCF 2020 SURVEY



Общие проблемы с K8s

КАКОВЫ ВАШИ ТРЕБОВАНИЯ? ГДЕ У ВАС ТРЕДНОСТИ?

Видимость и понимание

Безопасность

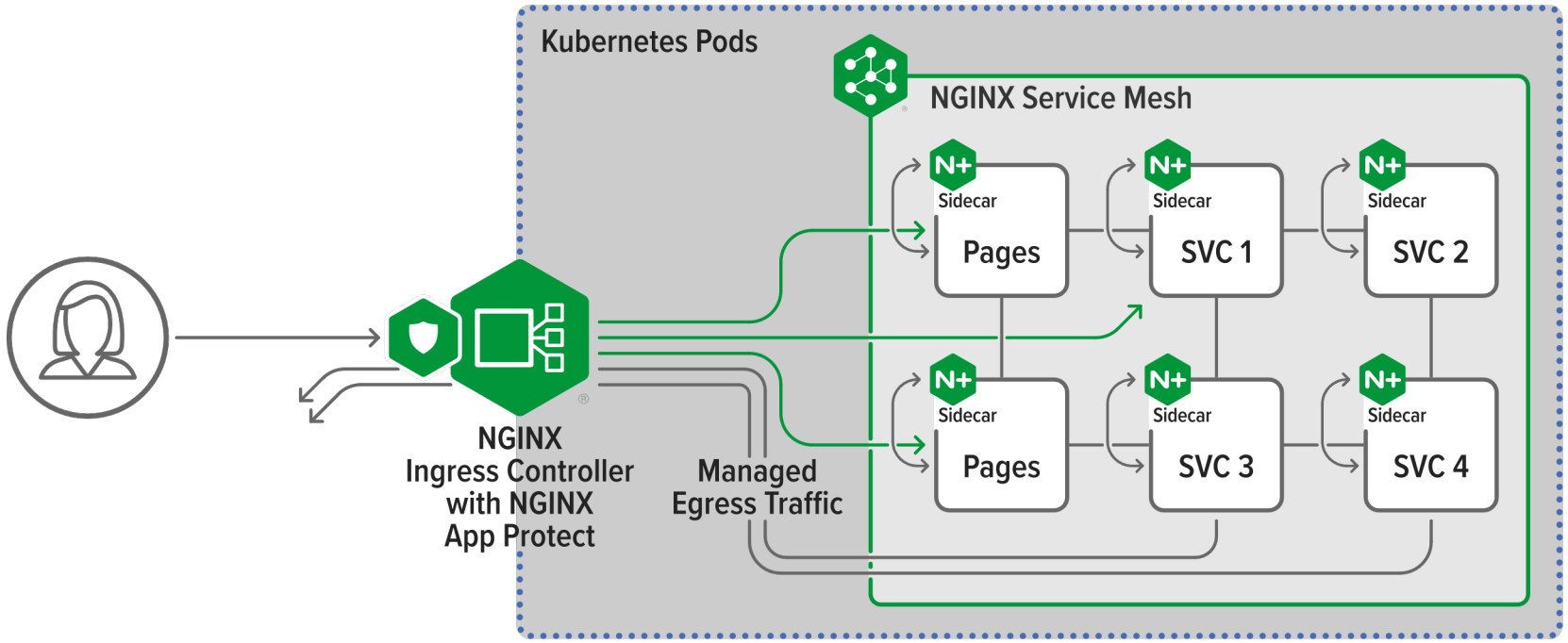
Масштабируемость

Kubernetes промышленного уровня с NGINX

Часть 1: Ingress Controller

Часть 2: Built-In Security

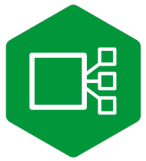
Часть 3: Service Mesh



Почему не стоит использовать community версию NGINX Ingress Controller

ПОДОЖДИТЕ, ИХ БОЛЬШЕ ОДНОЙ?

Инновации за счет стабильности функций



NGINX Ingress Controller®

Стабильность Enterprise уровня
без ущерба для инноваций

Размер

Community: 500MB
NGINX Plus: 120MB

Задержка

Community: Slowed by timeouts
NGINX Plus: Dynamically reconfigures

Timeout

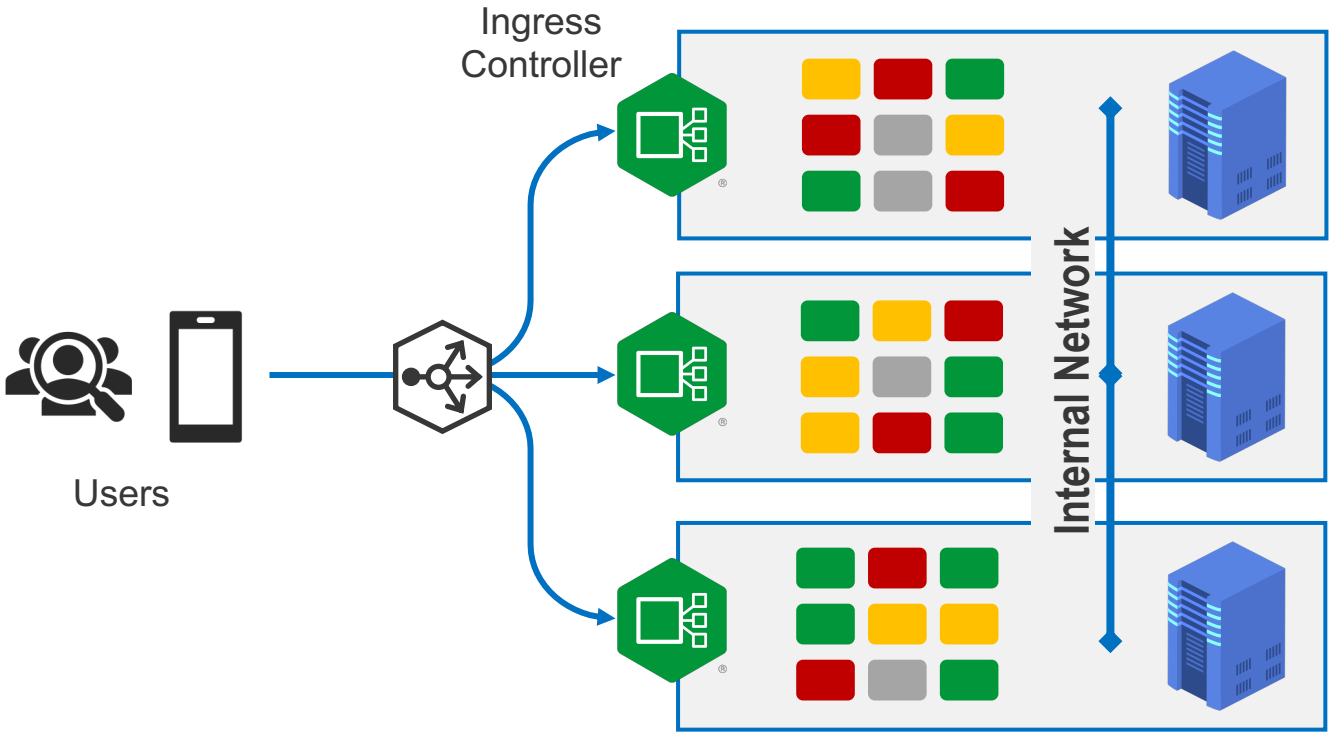
Community: 8809
NGINX Plus: 0

Защита

Community: OpenResty = CVE problems
NGINX Plus: Proactive CVE patching, Integrated WAF & service mesh

The Ingress Controller

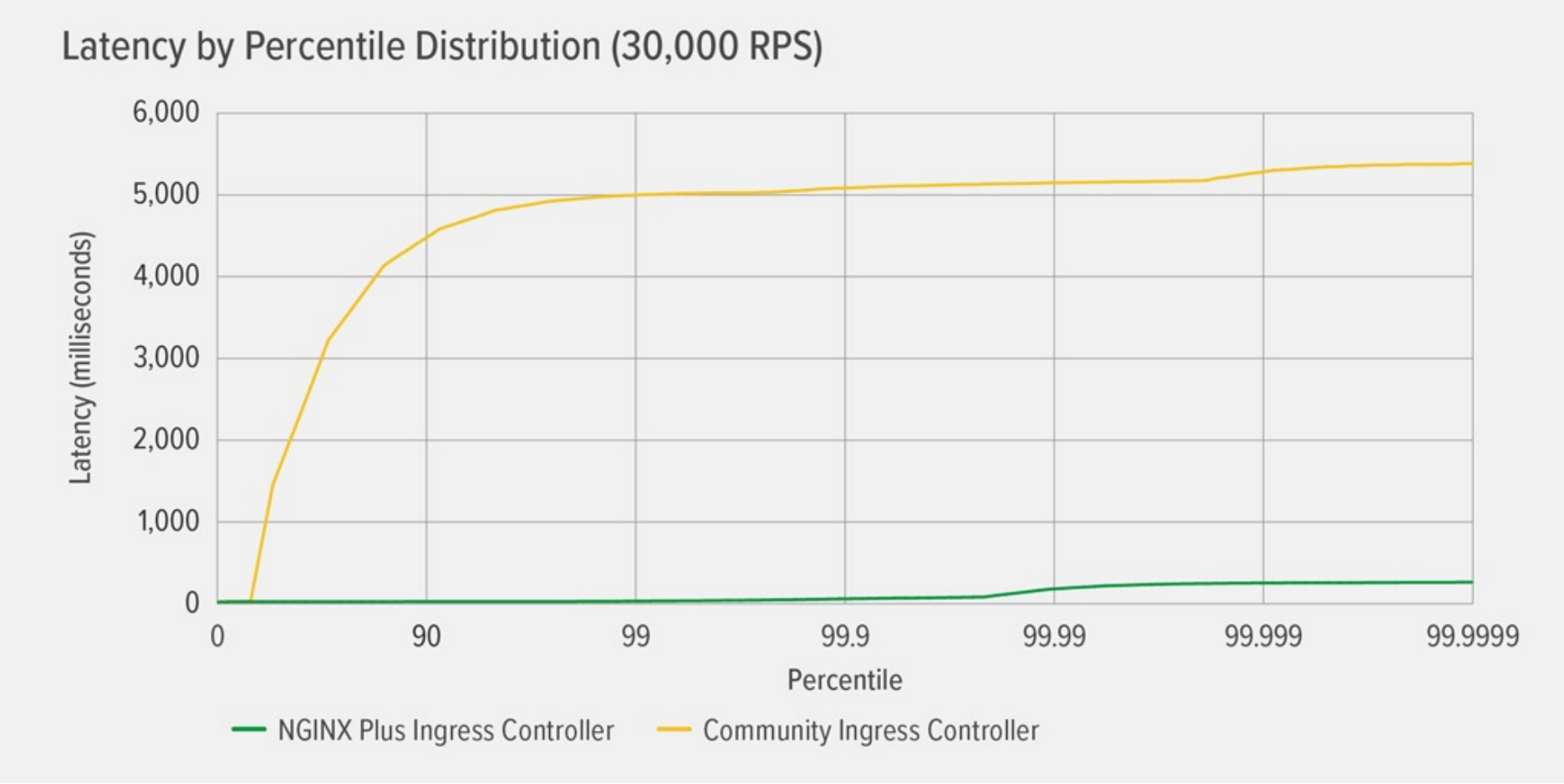
Специализированный балансировщик нагрузки для сред Kubernetes:



- Принимает трафик извне платформы Kubernetes и распределяет его по подам (контейнерам), работающим внутри платформы.
- Настраивается с помощью Kubernetes API, с объектами, называемыми «Ingress Resources».
- Контролирует поды, запущенные в Kubernetes, и автоматически обновляет правила балансировки нагрузки, например, если поды добавляются или удаляются из сервиса.

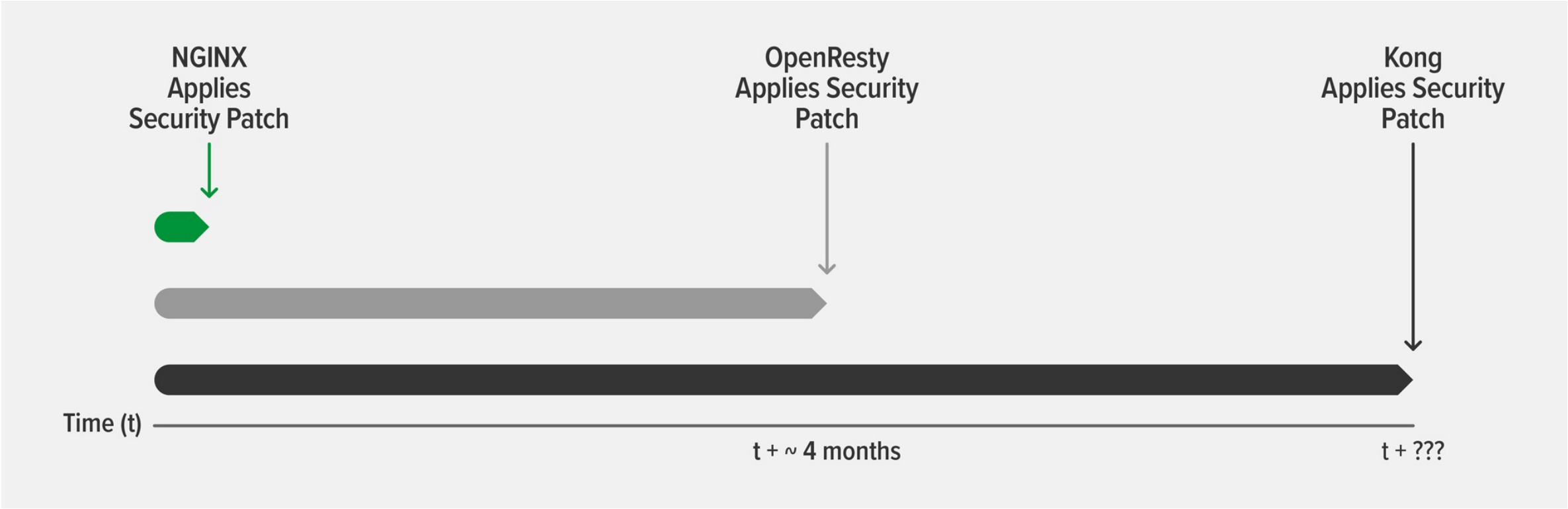
Задержка при динамическом развертывании

РЕЗУЛЬТАТЫ ТЕСТОВ ПРОИЗВОДИТЕЛЬНОСТИ 2020 ГОДА



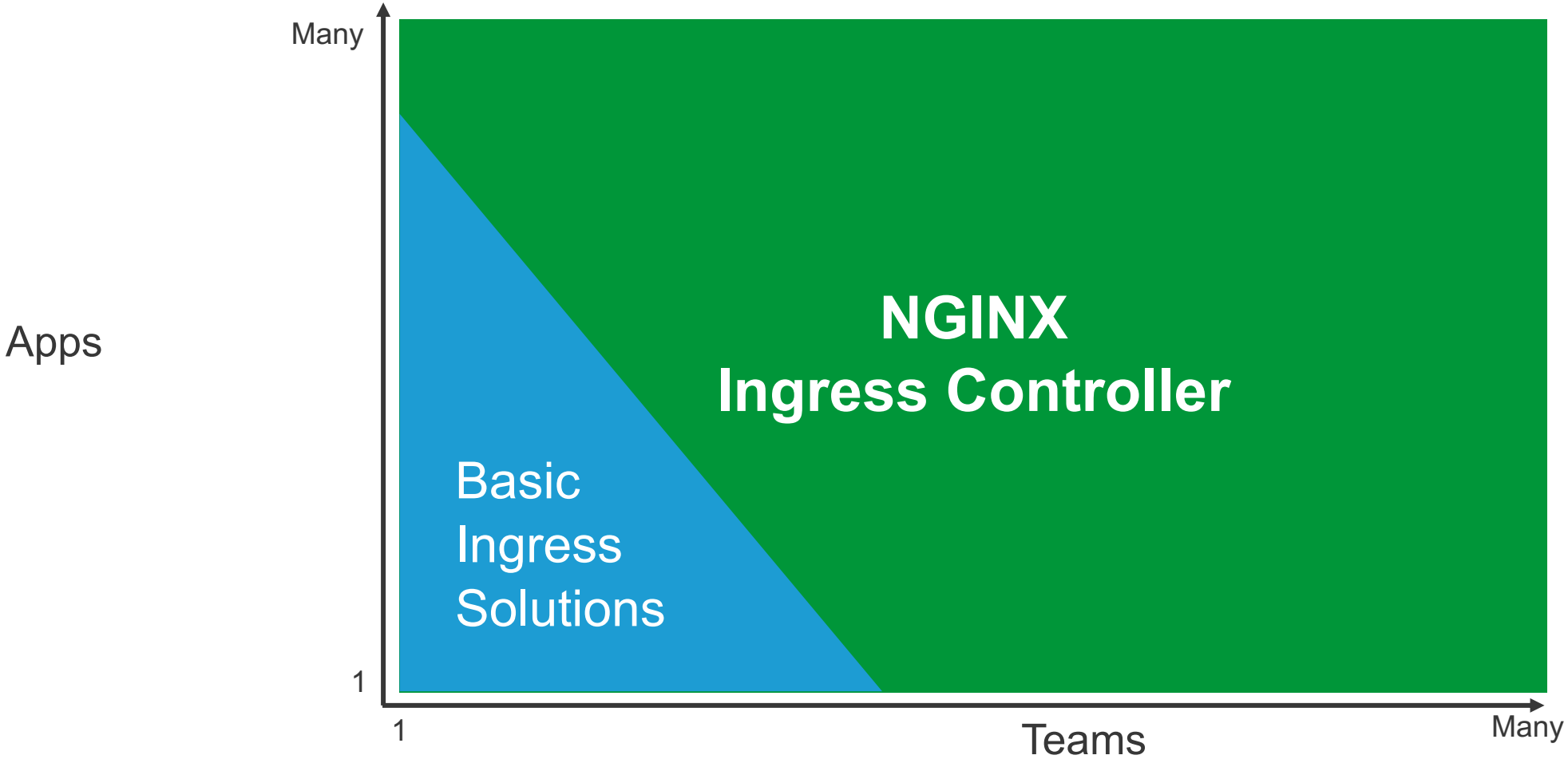
Задержки в исправлении CVE

ИЗЛИШНИЙ РИСК В ВАШЕЙ СРЕДЕ K8S



Manage Complexity in Production

WITH KUBERNETES & NGINX INGRESS CONTROLLER



Две проблемы при промышленном использовании

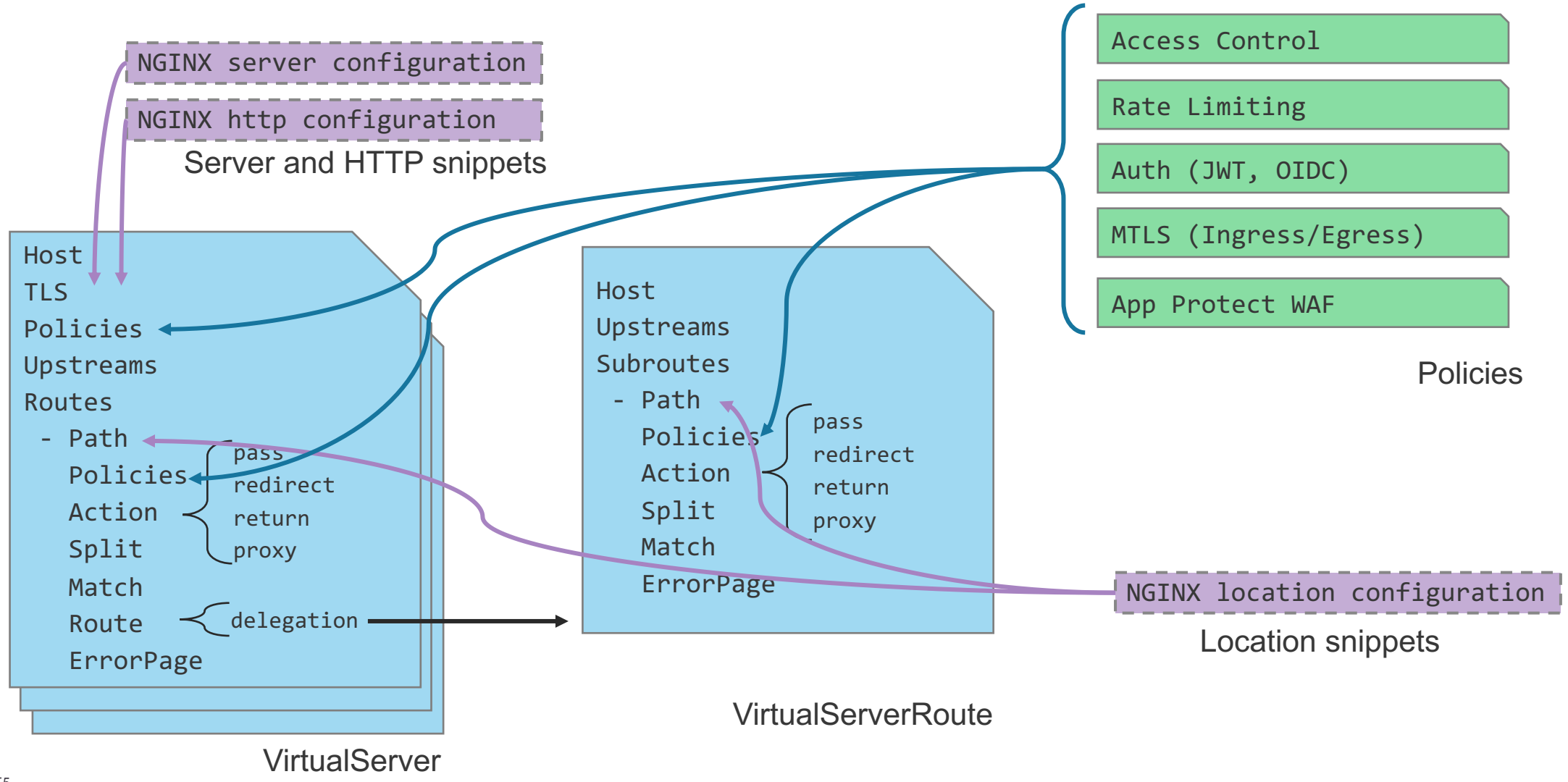
Сложные приложения

Как вы можете предоставить расширенные возможности, необходимые для сложных приложений?

Множество команд

Как несколько команд и приложений могут безопасно и совместно использовать контейнерную среду ?

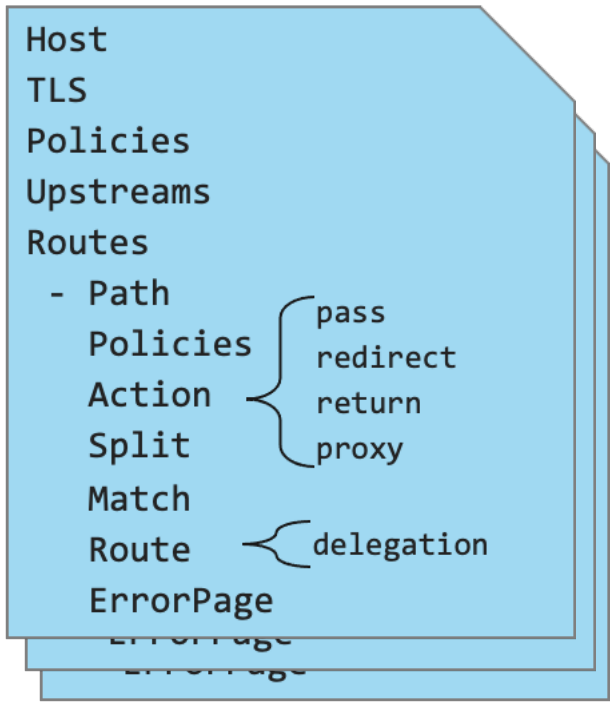
NGINX Ingress Resources – Богатые возсожности

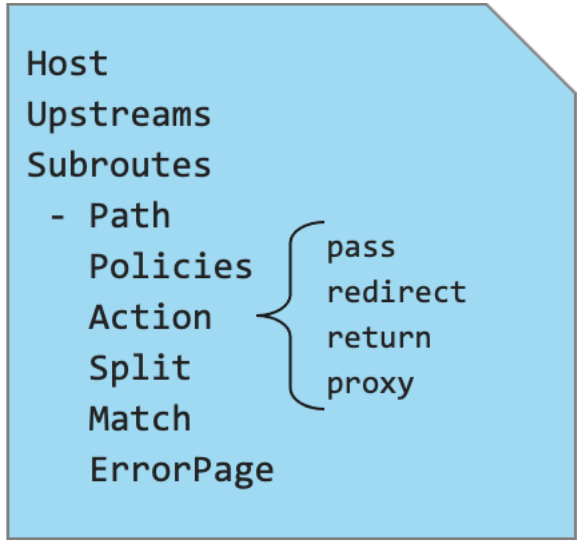


Некоторые примеры использования

Conditional Routing	→	*Несколько версий, несколько клиентов*
Split Routing	→	*A|B тестирование для развертывания в проде*
Error Pages	→	*‘Circuit Breakers’ для устранения отказов*
Rate Limiting	→	*Защита уязвимые приложения*
Authentication	→	*Выгрузить прерку логина из приложений*
Web Application Firewall	→	*Защита от уязвимостей*
NGINX Snippets	→	*“привычная” конфигурация NGINX*

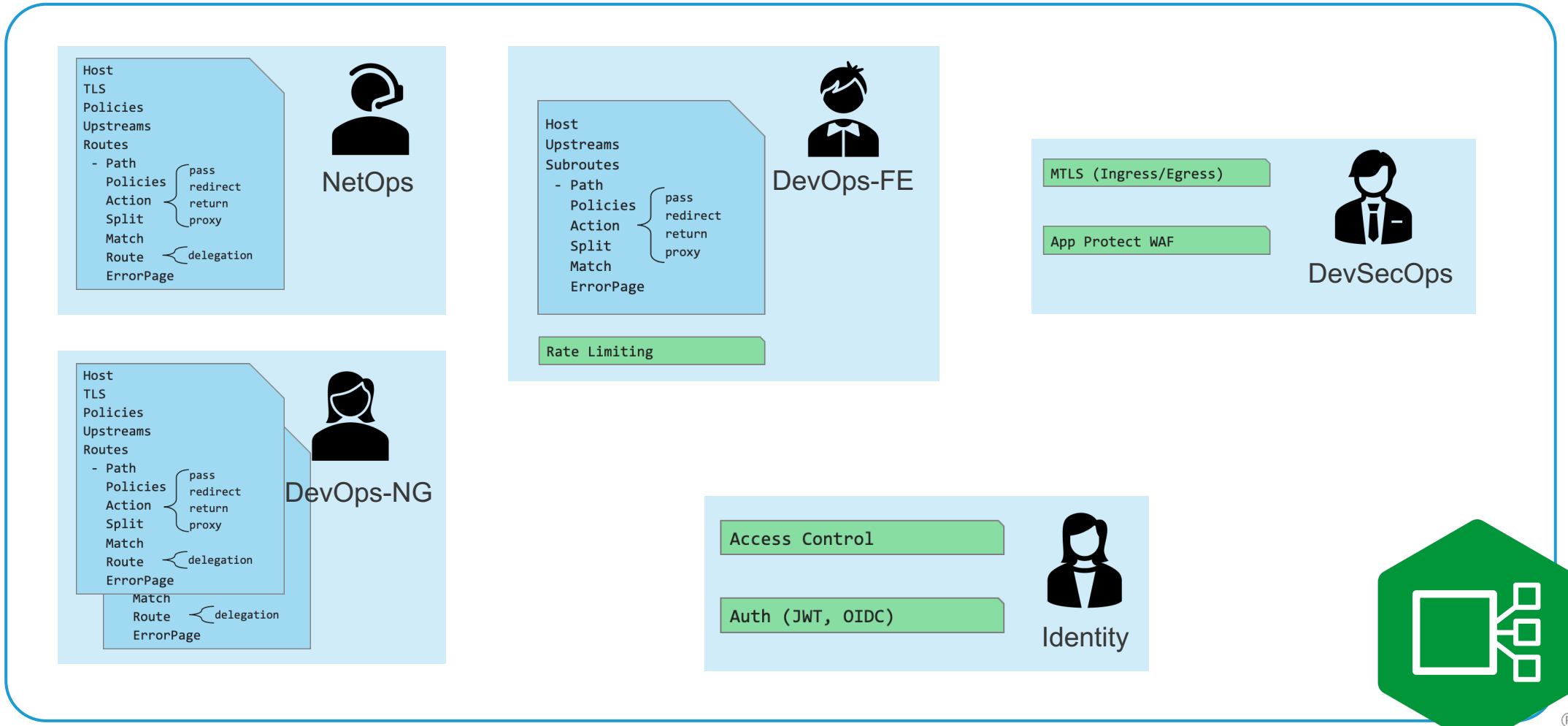
NGINX Ingress Resources – распределенная настройка





- Access Control
- Rate Limiting
- Auth (JWT, OIDC)
- MTLS (Ingress/Egress)
- App Protect WAF

NGINX Ingress Resources – распределенная настройка



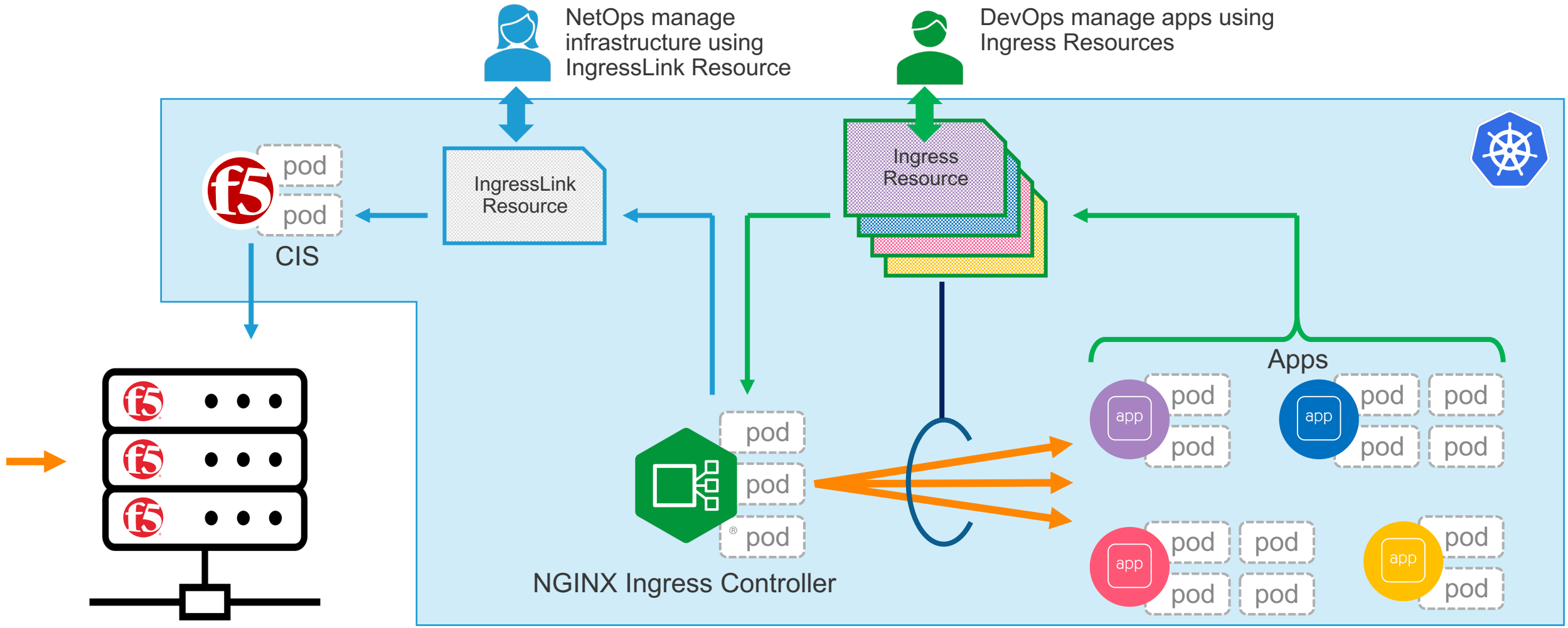
У DevOps и NetOps разные предпочтения

87% ПРЕДПРИЯТИЙ, ОПРОШЕННЫХ F5, ИСПОЛЬЗУЮТ КАК СОВРЕМЕННЫЕ, ТАК И ТРАДИЦИОННЫЕ АРХИТЕКТУРЫ.

	DevOps	SecOps / NetOps
Ответственность	Отвечает за указанные приложения и услуги	Отвечает за широкую платформу, используемую для доставки нескольких приложений
KPI	Инновации и гибкость - двигайтесь быстро и ломайте привычные вещи	Предсказуемость и безопасность - 100% время безотказной работы
Технологии	L7 и выше. L4 ниже – это “колдунство”.	L7 и ниже. То, что происходит выше, - это чья-то еще проблема
Типы систем	Программное обеспечение, в контейнерах или пакетах Linux	Автономные устройства, виртуальные или аппаратные
Управление	Автоматизация, API	Скрипты CLI / GUI или API
Безопасность	Хорошо иметь контакт с командой ИБ	Полностью их зона ответственности

F5 Ingress Link

ПОЗВОЛЯЕТ КОМАНДАМ NETOPS И DEVOPS РАБОТАТЬ СО СВОЕЙ СКОРОСТЬЮ

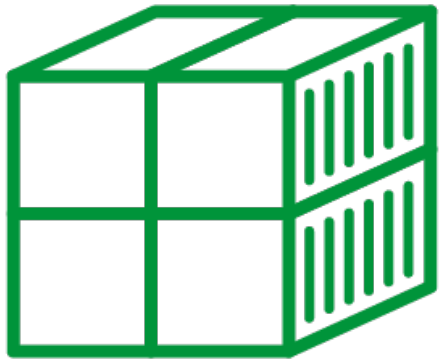


Trends and Challenges in Kubernetes

AGILITY VS SECURITY

70%

Will run containerized apps in production by 2023



94%

Experienced a security incident Kubernetes/container environments during the last year

44%

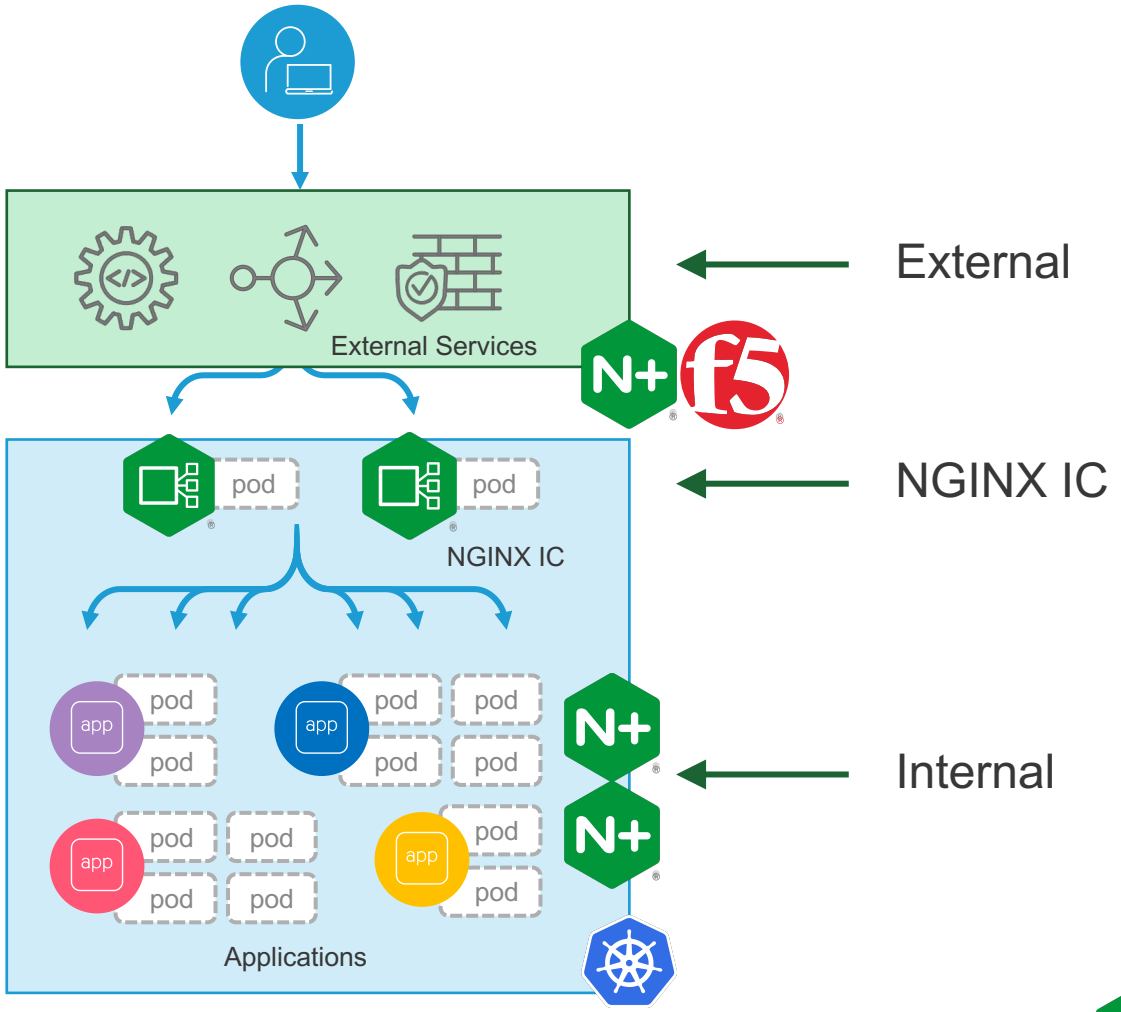
Delayed or halted containerized app deployment into production

Securing Kubernetes from the Inside

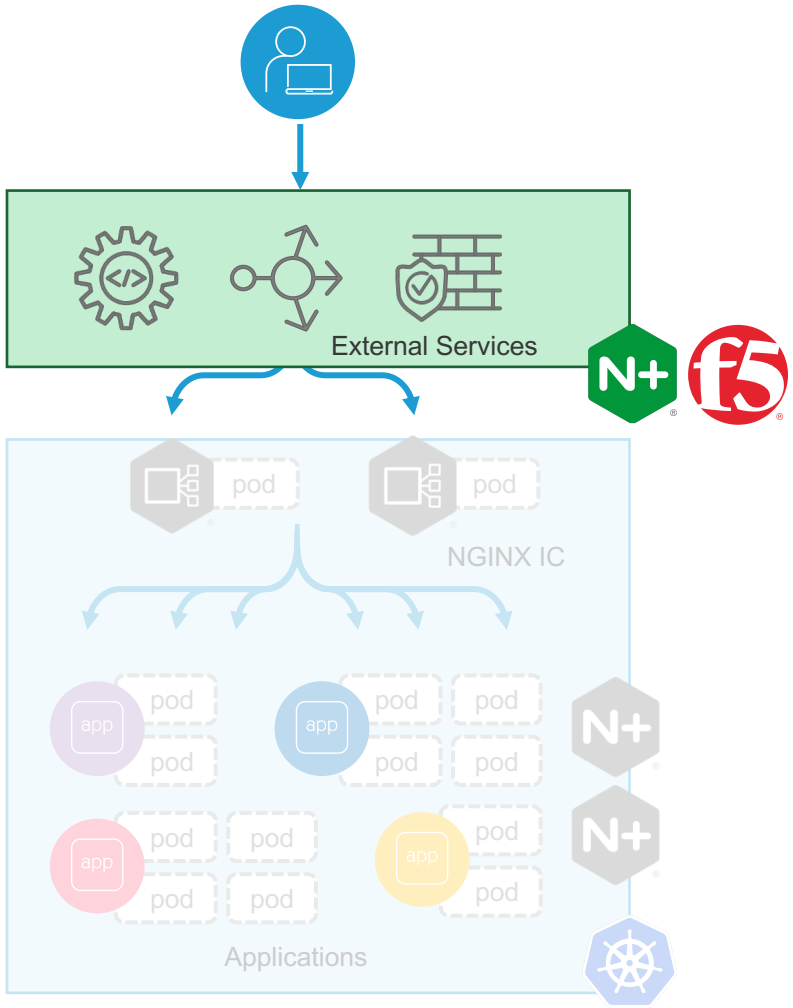
A DEVOPS STORY

Authentication and Authorization

Web Application Firewall



Deploy Security at the Edge



Appropriate for NetOps/SecOps-managed Security	
Primary User	**SecOps**
Scope	**Global**
Cost/Efficiency	**Good/Excellent (consolidation)**
Configuration	**BIG-IP, nginx.conf**

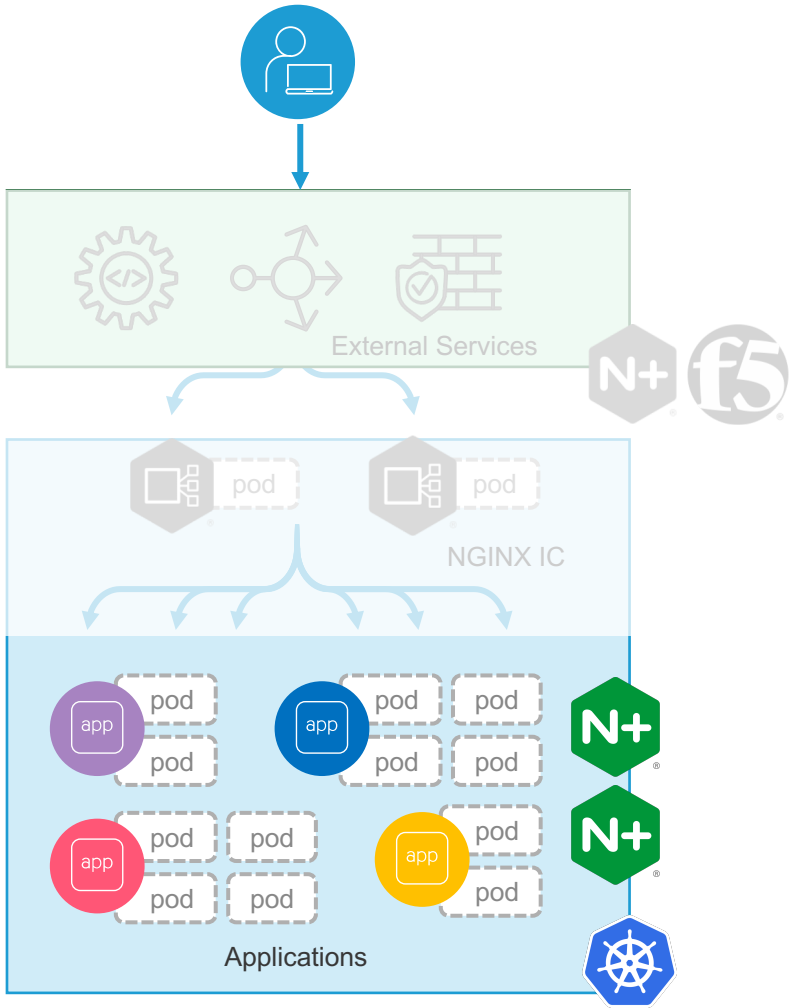
NetOps/SecOps-Centric Approach

This is a prime use case for edge services, external to K8s.

NetOps/SecOps manage security policies with a global outlook, with consistent governance for all applications.

Individual LoB teams need to defer to central IT for all matters relating to security.

Deploy Security with the Application



Appropriate when AppOwner has full control over security	
Primary User	**AppOwner/DevOps**
Scope	**Per-service or Per-endpoint**
Cost/Efficiency	**Often poor**
Configuration	**GitHub and nginx.conf**

Fine-grained per-Application Approach

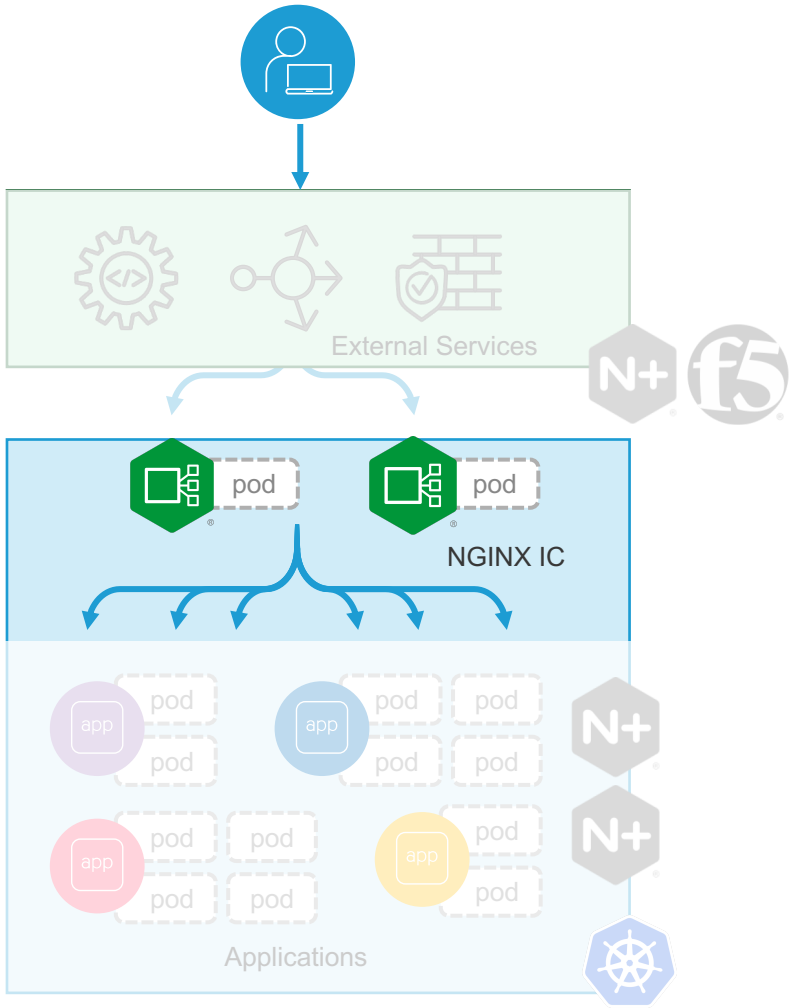
Appropriate solution when App Owner has full control of security for their application.

Security is implemented using a service proxy or embedded proxy.

Implemented, tested and deployed using CI/CD pipeline; security require re-deployment of application pods

Suitable for services that require very close control and testing of security configuration.

Deploy Security on the Ingress Controller



Appropriate for Kubernetes-native SecOps or DevSecOps	
Primary User	**SecOps/DevSecOps**
Scope	**Per-service or Per-URI**
Cost/Efficiency	**Excellent (high consolidation)**
Configuration	**K8s API**

Fine-grained per-Service or per-URI Approach

Perfect solution when security policies are under direction of SecOps or DevSecOps teams.

Policies are defined and associated with services using Kubernetes API.

NGINX Ingress Controller RBAC allows SecOps users to enforce policies per listener, DevOps users to select policy per Ingress Resource.

NGINX Ingress Controller и NGINX App Protect

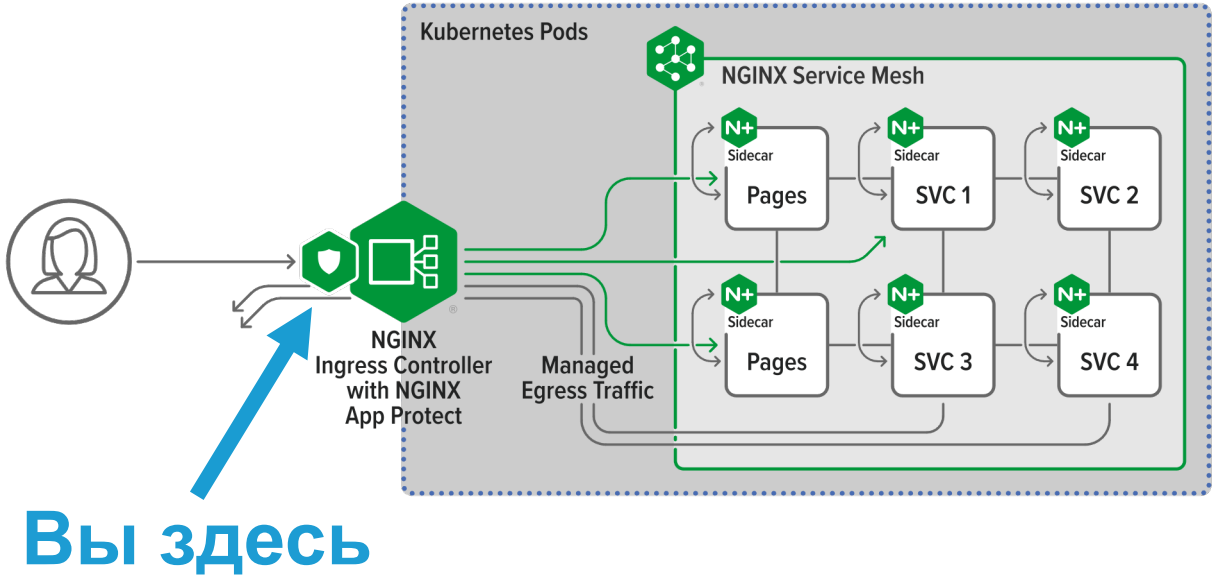
ЗАЩИТИТЕ ПРИЛОЖЕНИЯ БЕЗ ПОТЕРИ СКОРОСТИ

Полностью интегрированное решение

- Настраивается из знакомого мощного API K8s
- Встроенная в конвейер CI/CD безопасность и WAF

Преимущества для бизнеса

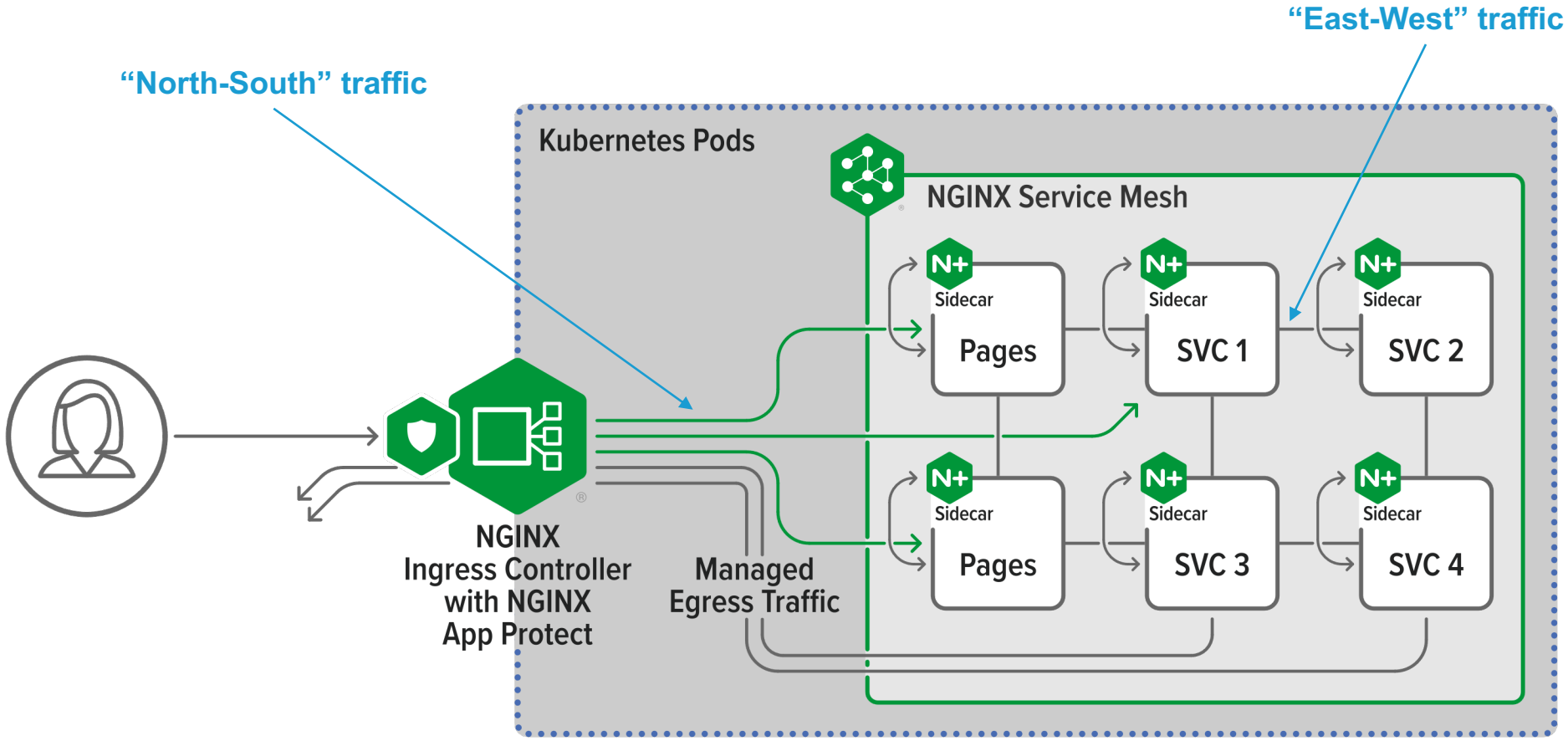
- Снижение сложности и разрастания инструмента
- Ускорение вывода на рынок и снижение затрат с помощью автоматизированной системы безопасности DevSecOps



Service Mesh

Где же находится service mesh

УПРАВЛЕНИЕ ТРАФИКОМ LAYER 7 В НАПРАВЛЕНИИ EAST-WEST



Что такое Service Mesh?

ЧЕГО НЕ ХВАТАЕТ В K8S И ЧТО ВАМ ДЕЙСТВИТЕЛЬНО НУЖНО И ЧТО НУЖНО ОТ MESH?

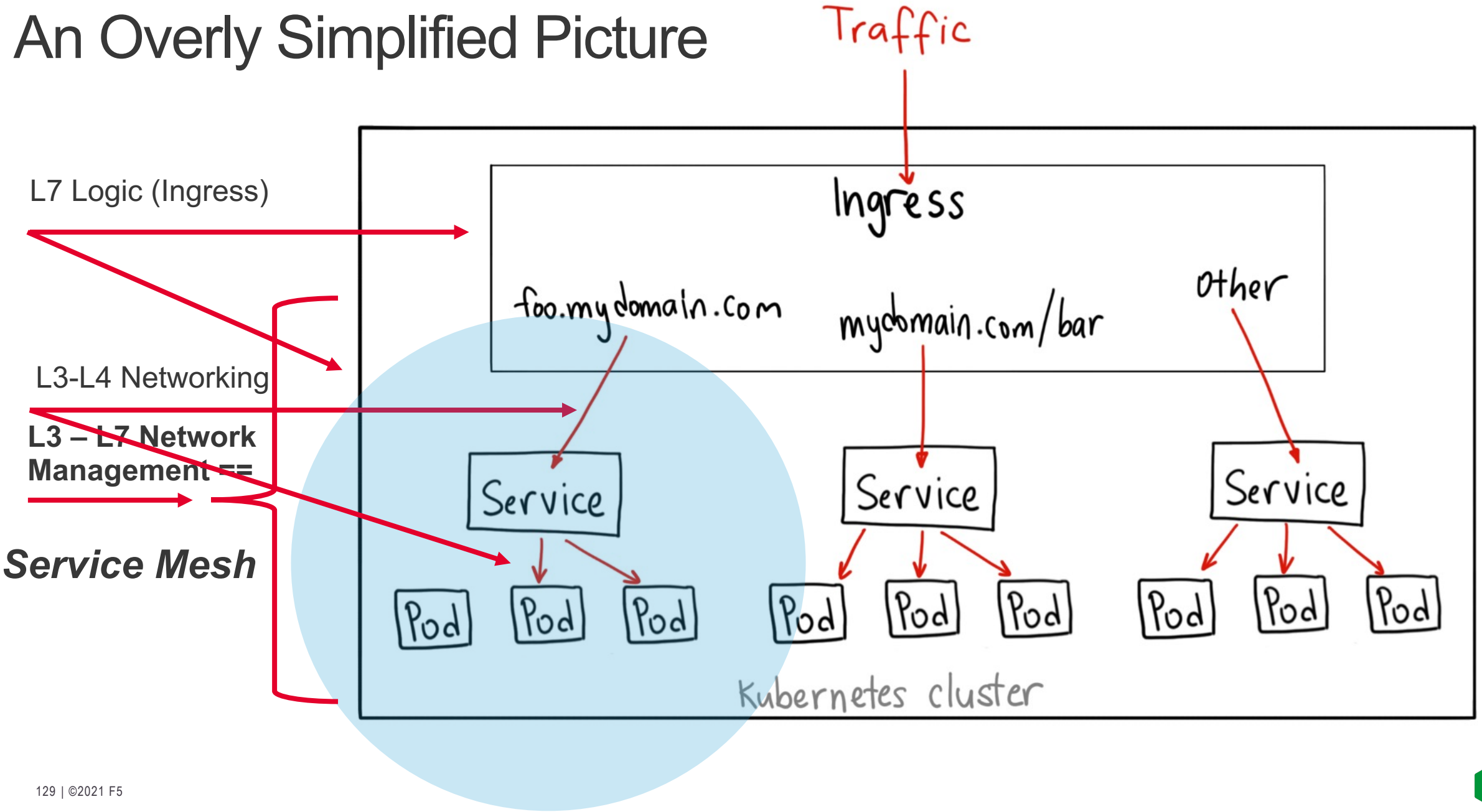
- Service mesh добавляет **управление трафиком L7** и его безопасность:
  - sidecar deployment
  - policy management
  - application availability/health,

- Service mesh - это не просто что-то одно, это множество управляемых и зависимых компонентов

- Включается, когда возможностей сети K8s не хватает (service/pod IP endpoints)

- ***“Управление трафиком для контейнеров”***

An Overly Simplified Picture



Некоторые примеры использования

Mutual TLS	→	*Безопасный трафик в сети с нулевым доверием*
Instrumentation	→	*Отслеживайте скорость, задержку и доступность*
Tracing	→	*Отладка транзакций и поиск неисправностей*
Rate Limiting	→	*Защита уязвимых приложений*
Traffic Splitting	→	*Применение A|B, Canary и Blue-Green обновлений*
Access Control	→	*Списки разрешений для управления трафиком*
Egress Control	→	*Управление трафиком на внешние сервисы*

Service Mesh Readiness Checklist

ЧЕМ БОЛЬШЕ УТВЕРЖДЕНИЙ ВЕРНО ДЛЯ ВАС, ТЕМ БОЛЬШЕ ПОЛЬЗЫ ОТ SERVICE MESH

1. У вас есть зрелый производственный конвейер CI / CD
2. Вы часто развертываете в производственной среде - не реже одного раза в день
3. Вы полностью интегрировали Kubernetes для своей производственной среды.
4. Ваше приложение сложно как по количеству, так и по глубине вложенности сервисов
5. У вас есть производственная среда с нулевым доверием, и вам нужен mTLS между сервисами
6. Ваша команда достигла операционной зрелости при развертывании и управлении приложениями, а это значит, что вам комфортно использовать Kubernetes в производственной среде, включая управление и поиск неполадок.

Selecting a Service Mesh

IT DEPENDS...

Why are you looking for a service mesh?

How will you use the service mesh?

What factors influence your selection?

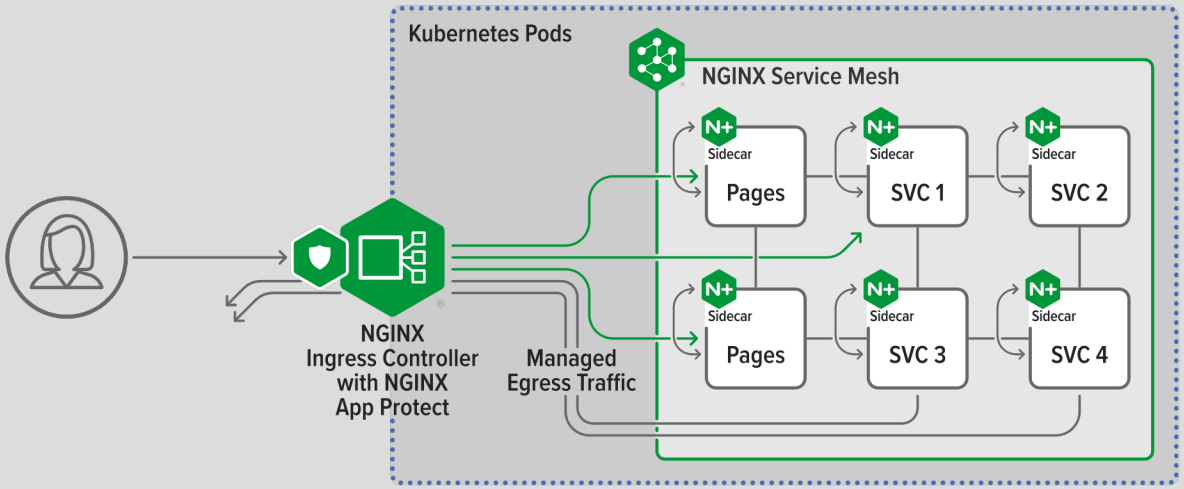
Чем вам понравится

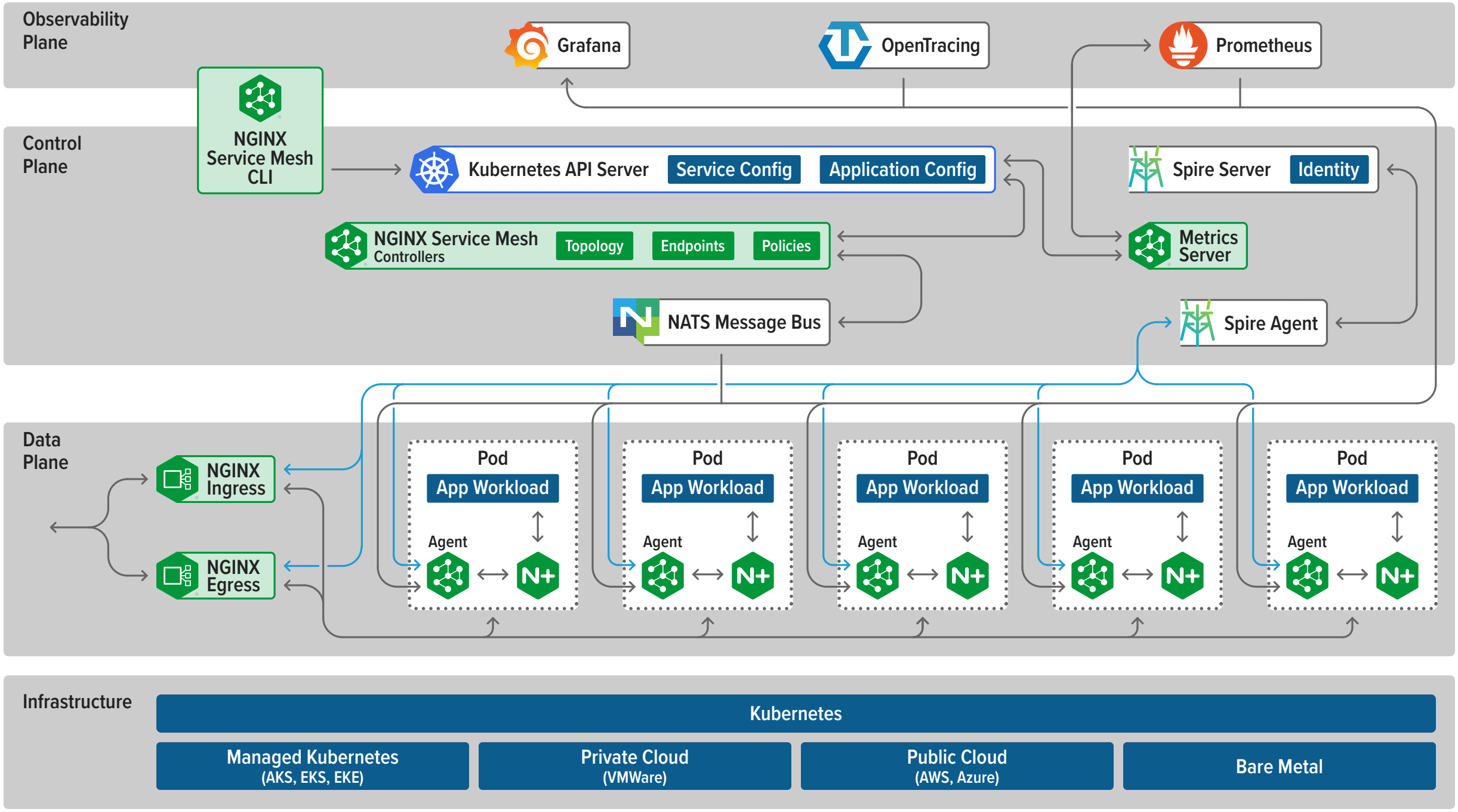
Удобство для разработчиков: Самообслуживание и простота использования, поэтому для его развертывания и управления не требуется команда специалистов по инфраструктуре. Никаких ручных настроек, основано на собственных инструментах Kubernetes и инструментах с открытым исходным кодом.

Мощный и эффективный : Самый быстрый и легкий способ получить mTLS и управление трафиком в среде микросервисов. Не нужно специальных компонент для NGINX Ingress Controller.

NGINX Plus Sidecar: Полностью интегрированная высокопроизводительная подсистема обработки данных для высокодоступных и масштабируемых контейнерных сред.

NGINX Service Mesh®




Observability Plane
Grafana
OpenTracing
Prometheus
Control Plane
NGINX Service Mesh CLI
Kubernetes API Server
Service Config
Application Config
Spire Server
Identity
NGINX Service Mesh Controllers
Topology
Endpoints
Policies
Metrics Server
NATS Message Bus
Spire Agent
Data Plane
NGINX Ingress
NGINX Egress
Pod
App Workload
Agent
N+
Infrastructure
Kubernetes
Managed Kubernetes (AKS, EKS, EKE)
Private Cloud (VMWare)
Public Cloud (AWS, Azure)
Bare Metal

Примеры использования NGINX Service Mesh

Основное отличие

Secure Traffic
End-to-end encryption (Mutual TLS / mTLS), ACLs

Лучший сайдкар на основе NGINX Plus

Orchestration
Injection and sidecar management, K8s API integration

Небольшая и эффективная система управления, удобство для разработчиков

Manage All Service Traffic
Load Balance, Circuit breaker, B|G, Rate Limiting…

Enterprise ADC sidecar на основе NGINX Plus

Visualize Traffic
Generate transaction traces and real-time monitoring

Спецификация SMI, открытая экосистема

Это все! …на сегодня

Время ваших вопросов!

NGINX®

Part of F5