Prevent downtime & breaches by securing your apps and APIs

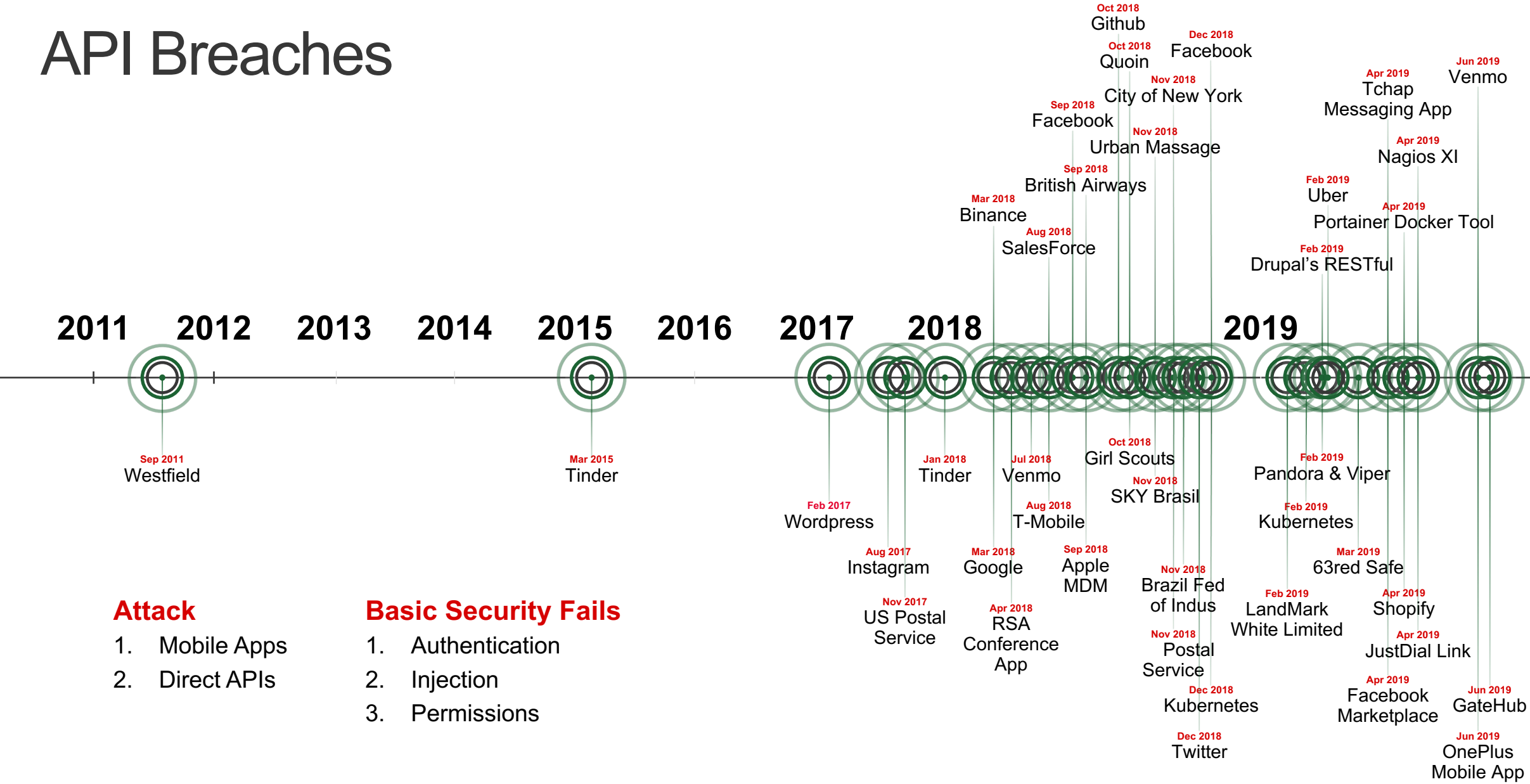
The Value of NGINX Plus

Koen Vanderpoorten
Solution Engineer BELUX

Agenda

- Introducing NGINX Plus
- Web Application Firewall
- API Management and security
- Kubernetes Ingress Controller
- Q&A

API Breaches



Attack

1. Mobile Apps
2. Direct APIs

Basic Security Fails

1. Authentication
2. Injection
3. Permissions

What keeps our customers up at night?

Security

Complex Operations

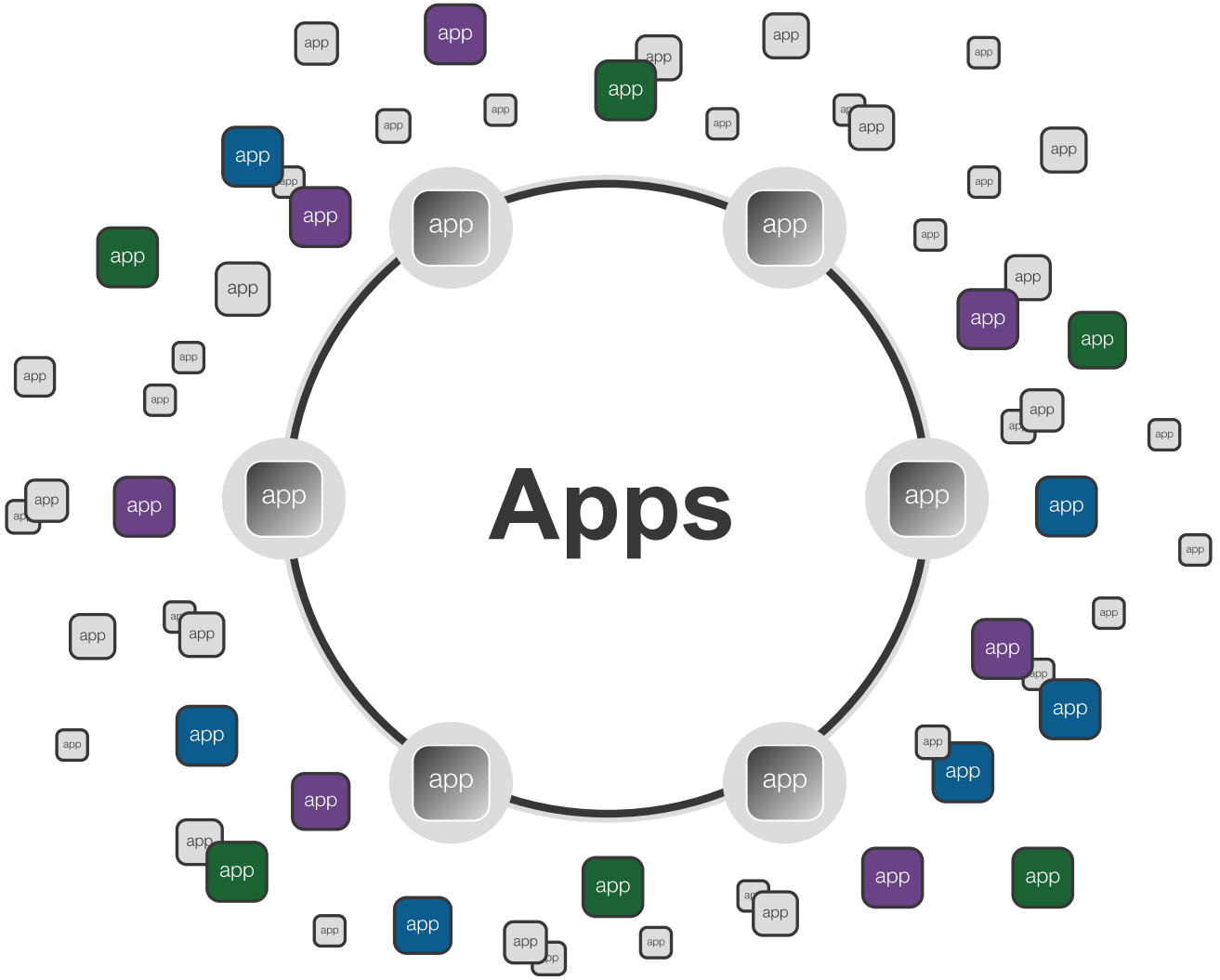
Cost

The Gateway to Data

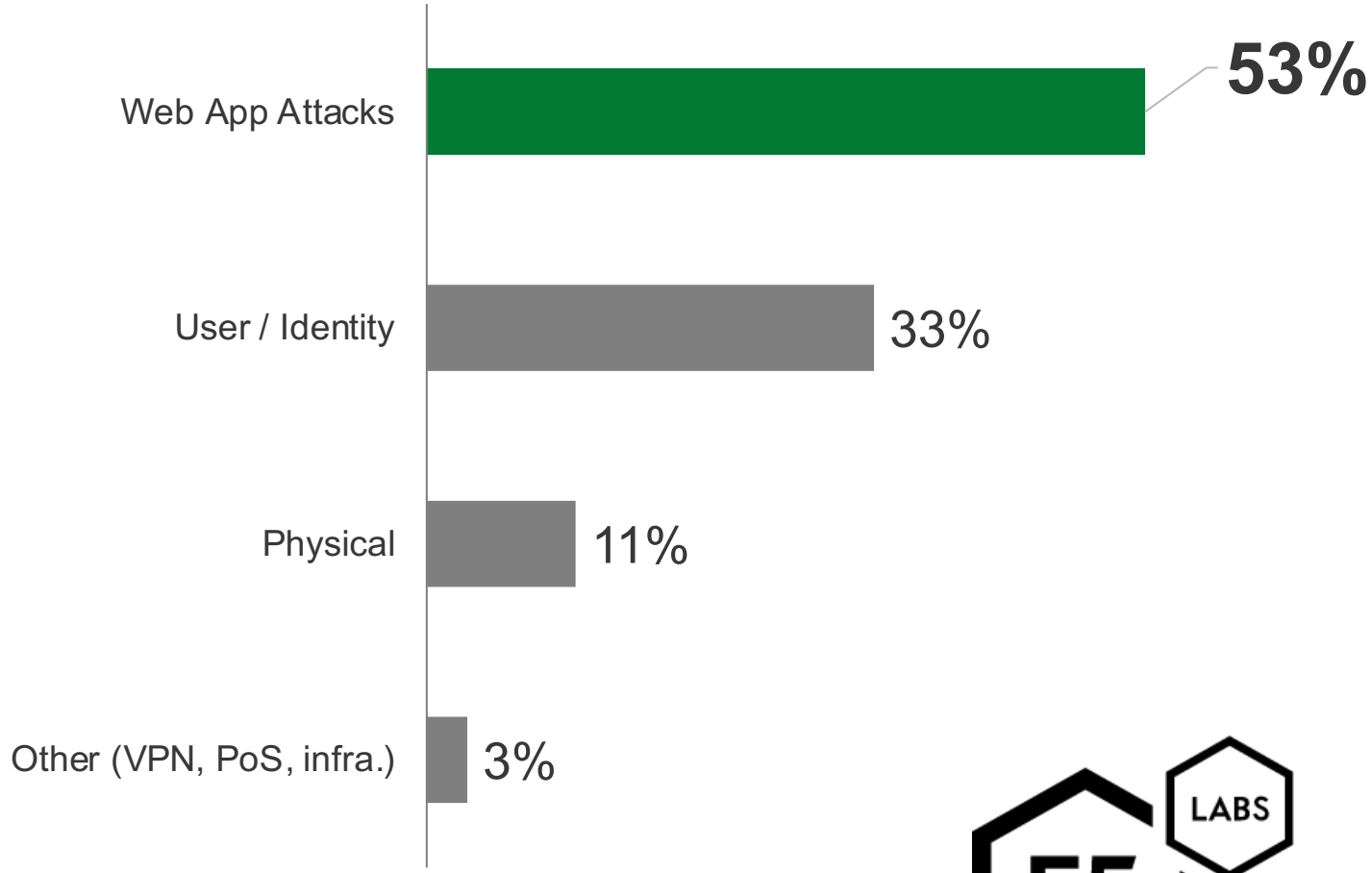
Average Enterprise

983

Apps in play



Apps continue to be the #1 attack target…



Software vulnerabilities & common attack vectors

SOFTWARE VULNERABILITIES IN APPLICATION STACKS (CVEs)

Software vulnerabilities are found in components of virtually all software stacks

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

FREQUENTLY OCCURRING WEAKNESSES IN APPLICATION CODE (OWASP Top 10)

Threats such as Injection and XSS are well known, but difficult to mitigate, thus remarkably common

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

REALITY: THE AGILE IMBALANCE

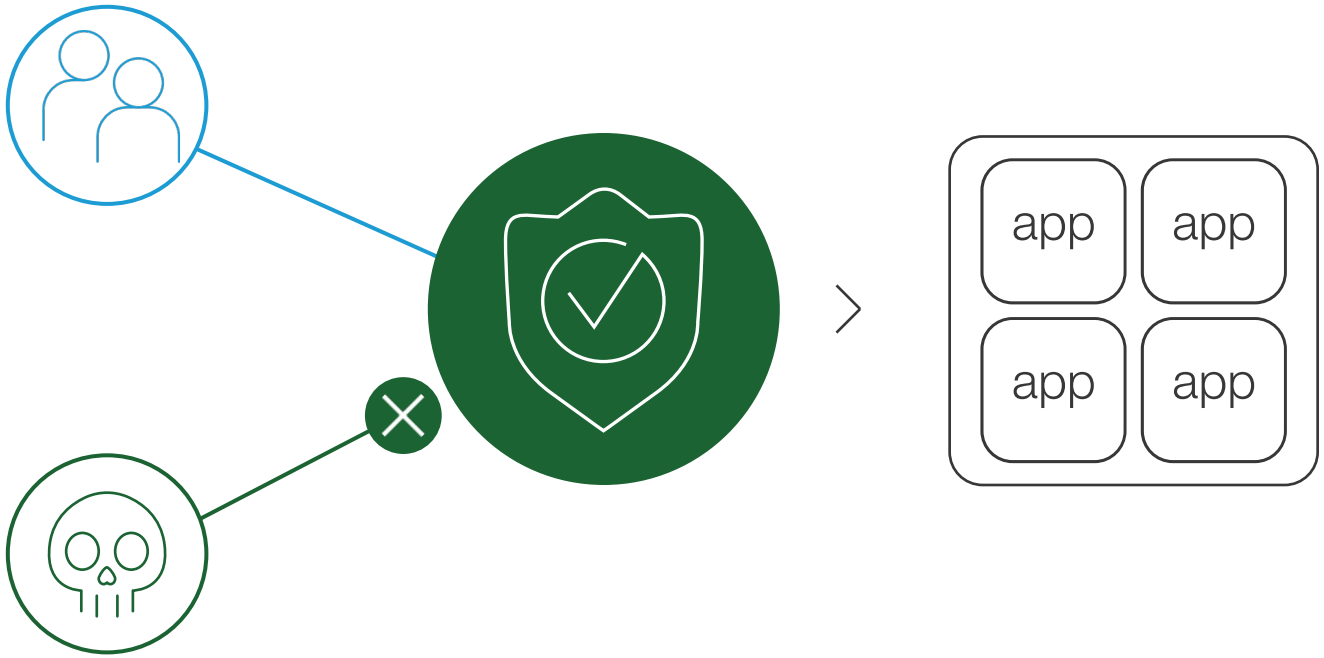
100	10	**1**
Developers	DevOps	**Security**

The Pipeline is Built for Speed, Not Security

"Waterfall" security policies often don't translate well to Agile and cloud environments

Security control objectives can't be adequately applied and enforced

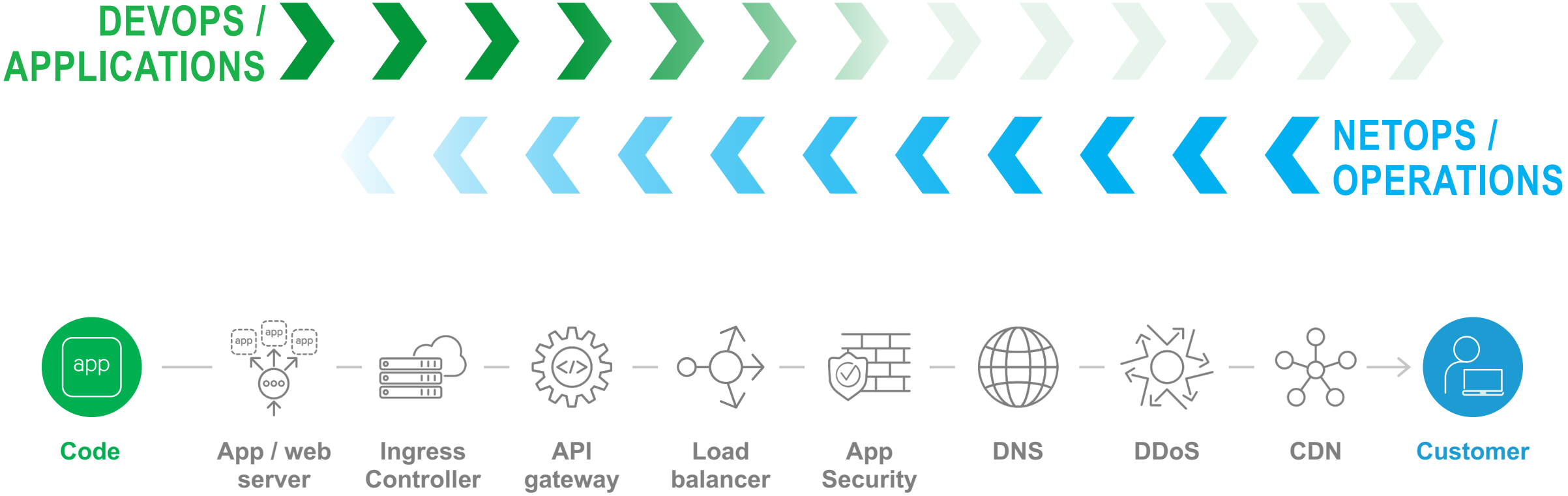
How do you protect apps?



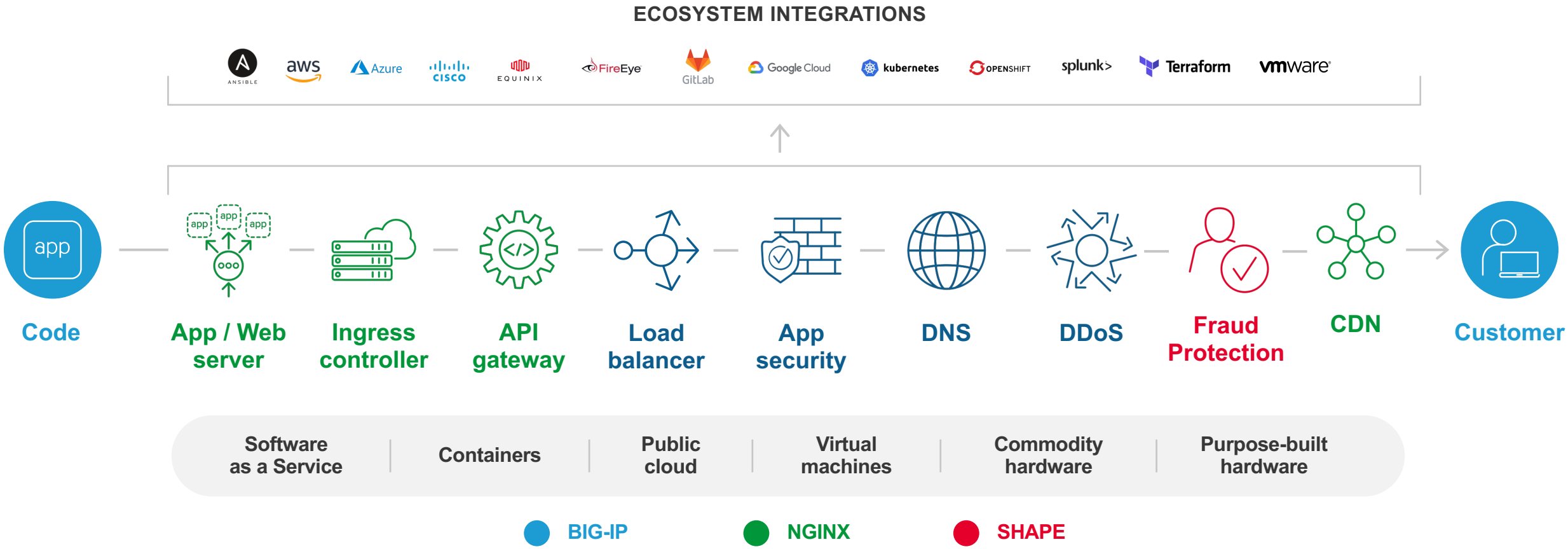
- Vulnerabilities
- Active attacks
- Risk and address compliance

Application Services

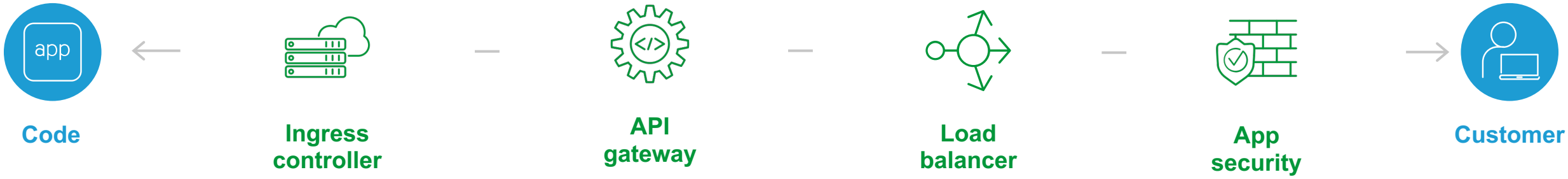
MAKING AN APPLICATION SECURE, RESPONSIVE AND ALWAYS AVAILABLE



F5 Portfolio

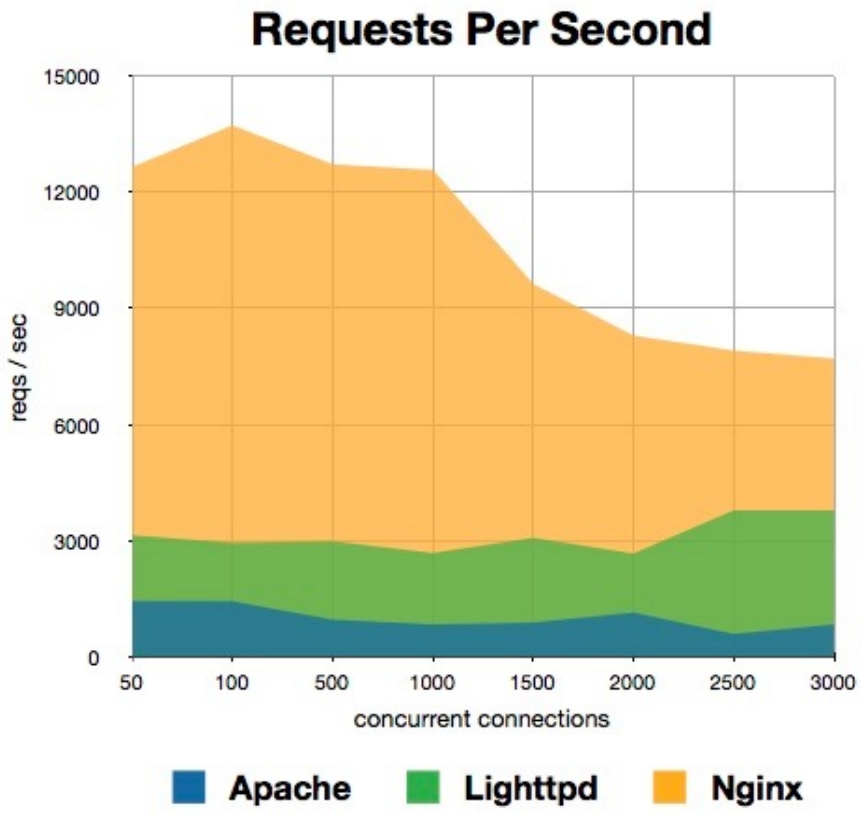


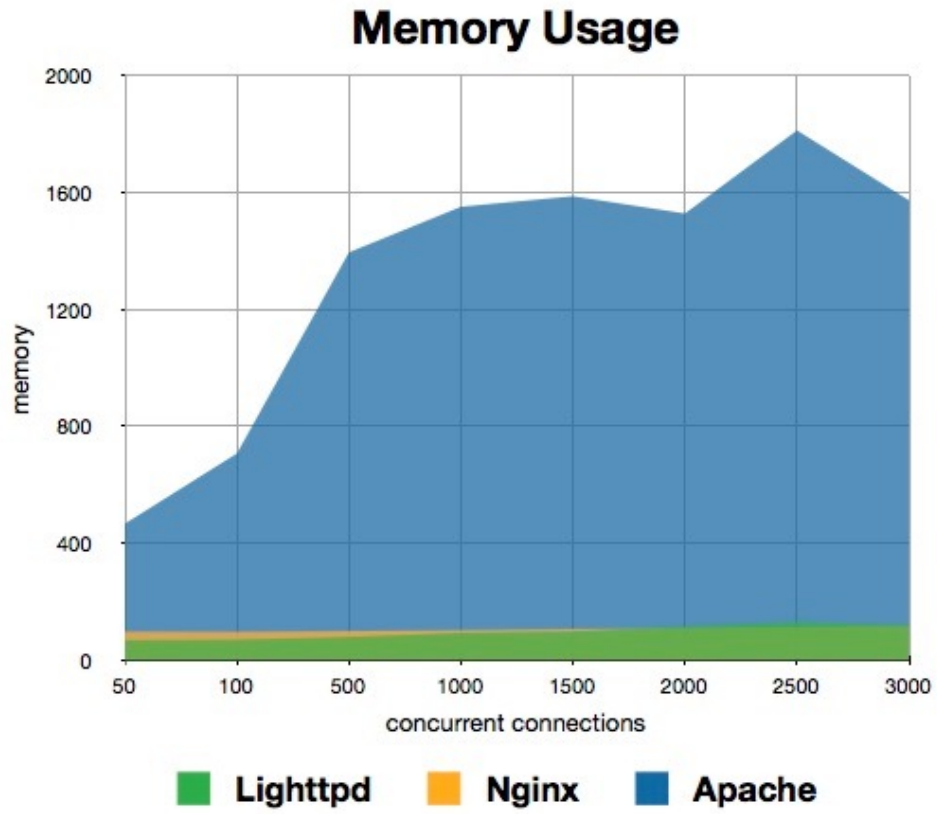
NGINX Use Cases



NGINX: fit for a modern environment

Tiny Memory Footprint
(< 1.4 Mb space optimized)
Microsecond startup time
Low-latency-optimized
Highly SMP Scalable
Multi-10Gbit throughput

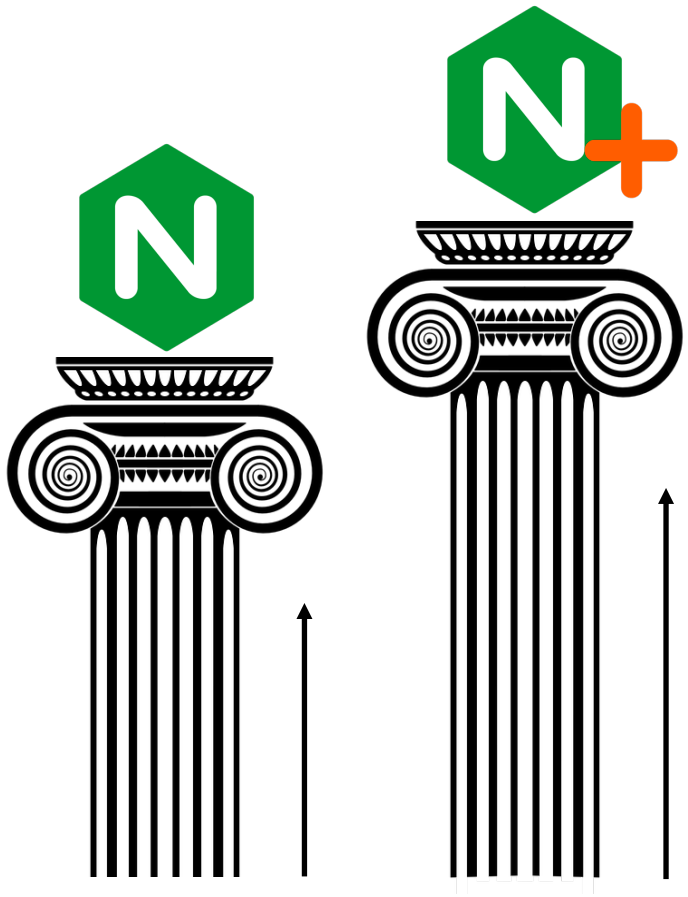




NGINX OSS vs NGINX Plus

NGINX open source

HTTP2
JSON Logging
Stream Module (TCP… UDP)
Multi Datagram UDP Support
Thread Pools
Dynamic Modules
JavaScript Module for NGINX
ECC Certificate Support
Linux Enhancements



NGINX Plus

All of Core Plus:
+ Authentication
+ High Availability
+ Web App Firewall (NGINX App Protect)
+ Centralized Management (NGINX Controller)
+ App Performance Analytic
+ K8S Services Discovery
+ API configuration
+ Enterprise-level supports within 30 minutes
+ First-priority CVE response

NGINX App Protect

F5 NGINX App Protect

Strong App Security

Built for Modern Apps

CI/CD Friendly

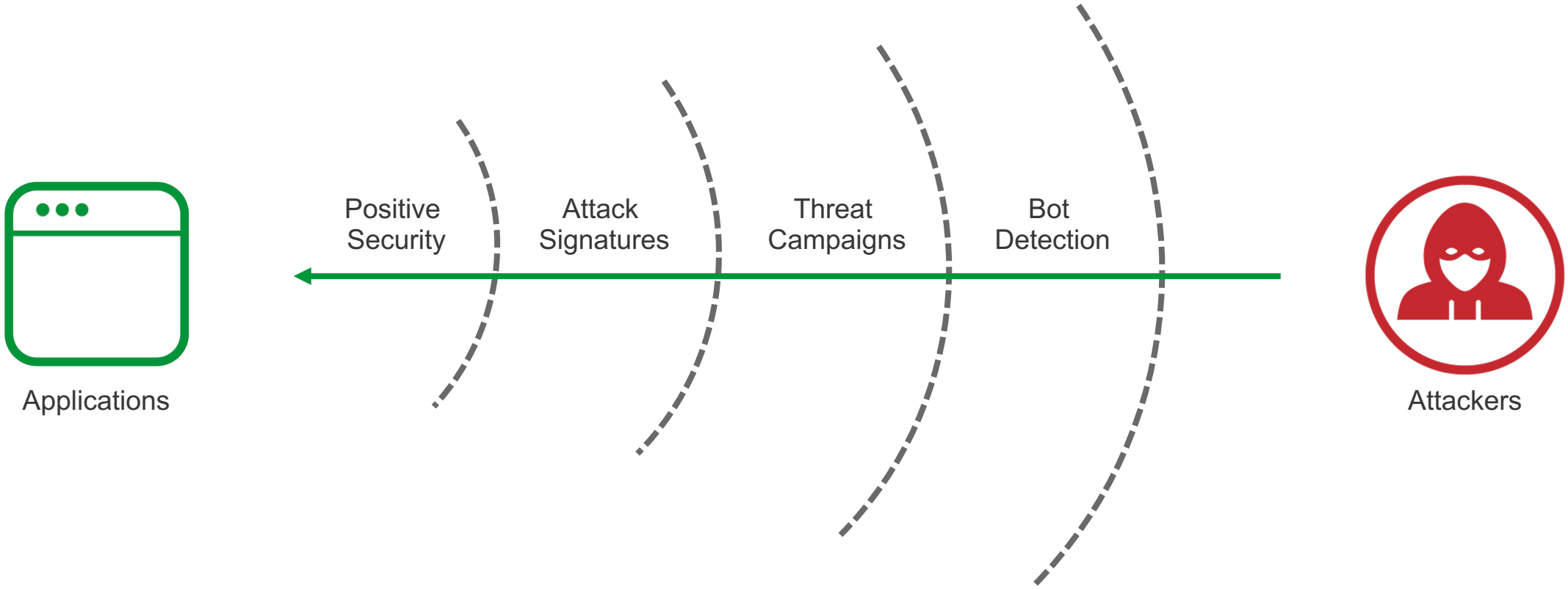
Strong App Security

App security and controls built using F5 advanced WAF technology. Blocks attacks and helps prevent downtime.

- **F5-based Layer 7 Attack Protection**
- **OWASP Top 10**
- **Regulatory Compliance**
- **API Security**
- **IP Blocking**
- **Prevent sensitive data loss**
- **Bot detection and Mitigation**
- **Layer 7 DDoS Protection**

NGINX App Protect - Strong App Security

A MULTILAYER APPROACH

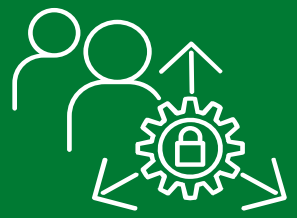


Built for Modern Apps

High performance security with performance and scale

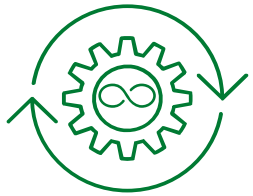
Seamless integration into the #1 web application platform

- **Seamless NGINX Integration**
- **High performance**
- **Deployment options**
- **Minimizes tool sprawl**
- **20X+ faster than alternative OSS**
- **Lightweight footprint**



CI/CD Friendly

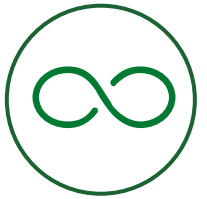
Enable security to keep pace with DevOps and Support “shift left” initiatives



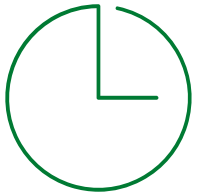
Automate security in CI/CD cycle

Enable AppDev

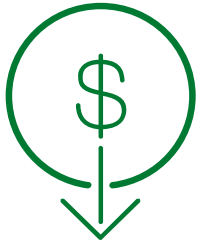
Declarative policies



Feedback loops

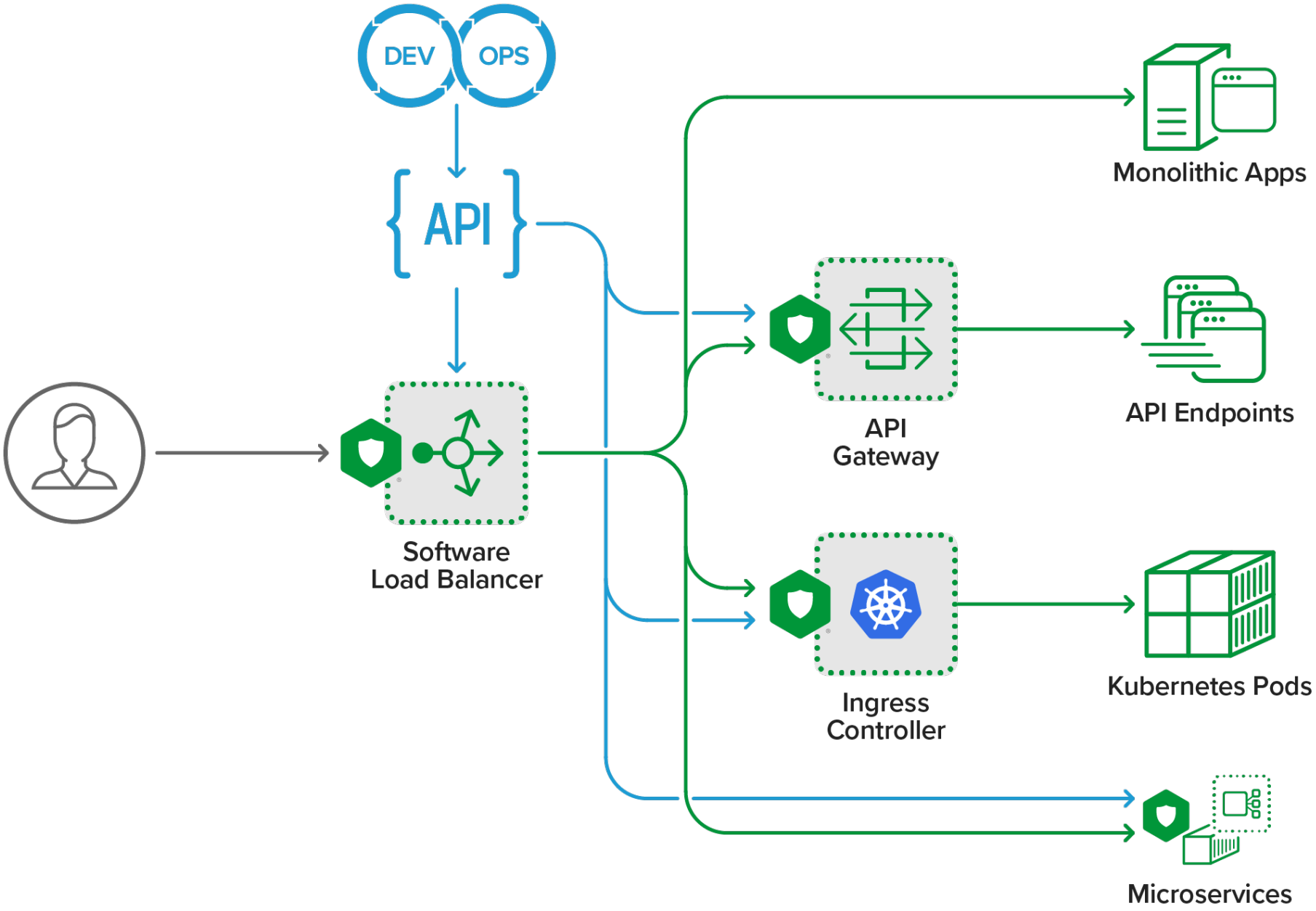


Speed Time to Market

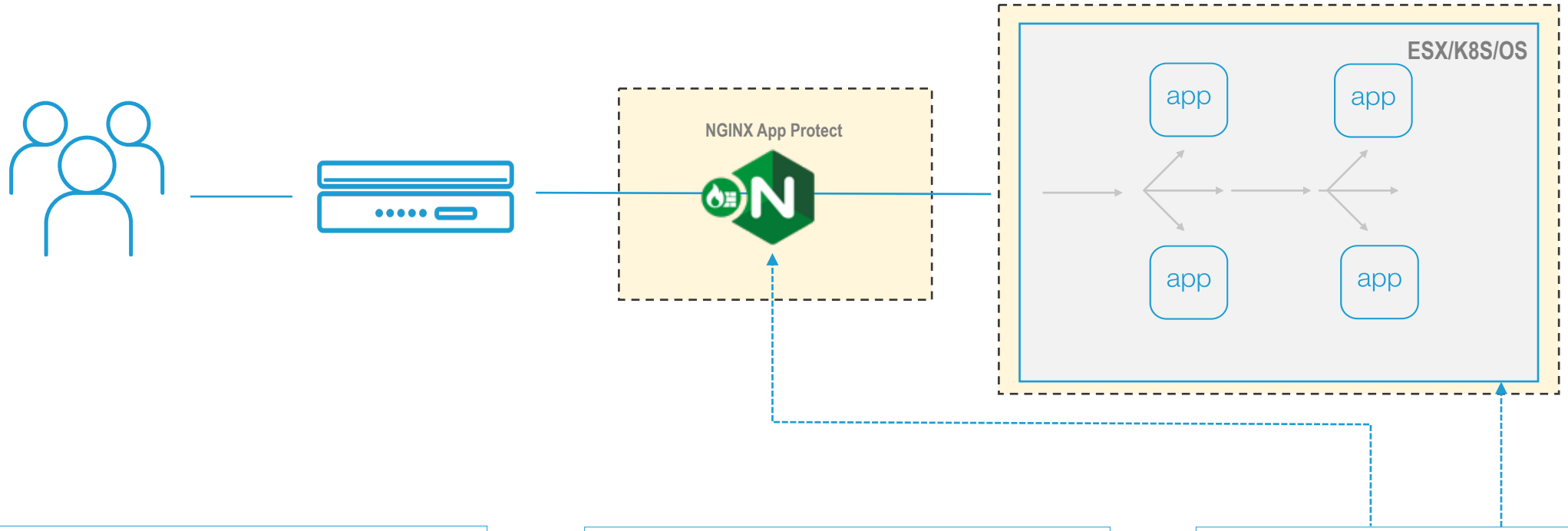


Reduced cost

Deployment options



App Services Automation with Open Source tools



GitHub **Source Code Repository**

Application code/config for API
ADC & Security policy/config for API

Jenkins **CI/CD Pipeline Tool**

Pipeline for build/test/deploy of API

ANSIBLE **IT Automation**

Ansible playbook for deployment of API with its App Services

NGINX API Management

Exposing you API – Key Areas for Consideration

SECURING APIs

APIs are HTTP and need protecting just like web traffic

API MANAGEMENT / GATEWAY

Control the scope and access to API endpoints

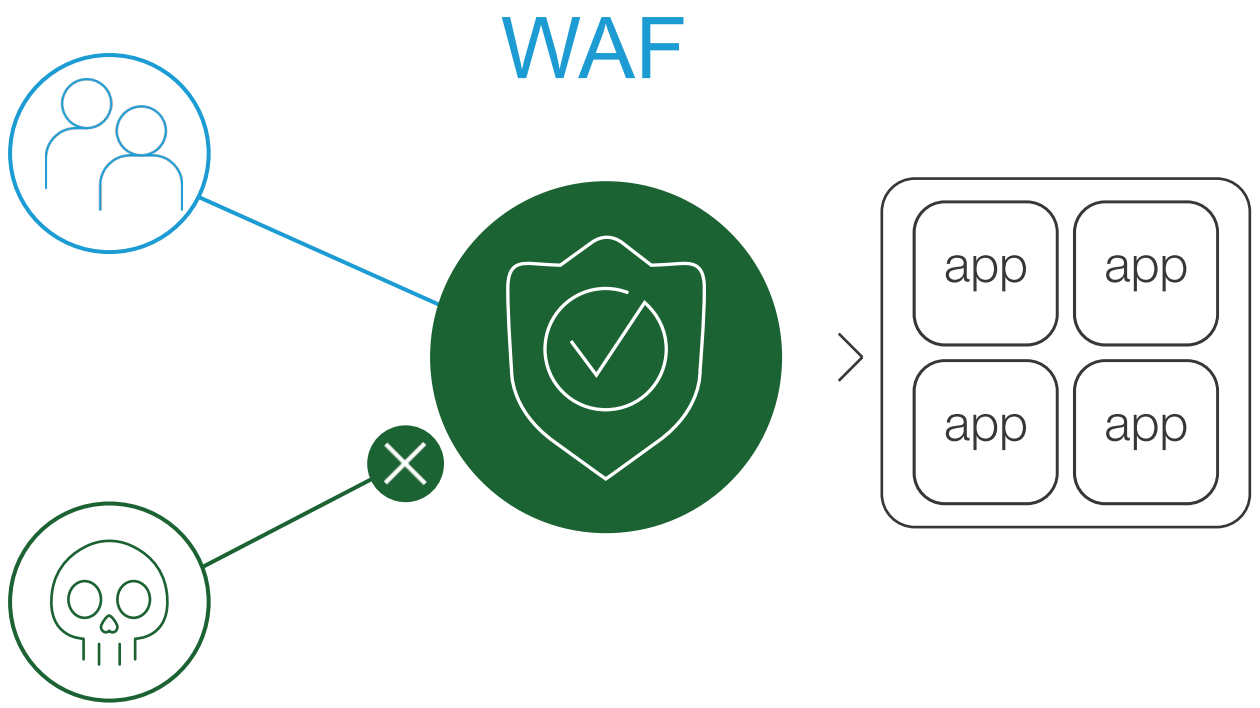
PERFORMANCE AND AVAILABILITY

Ensure API calls are delivered as fast as possible

API-focused secure application delivery

Key Area #1 – API Security

- Schema validation
- Protocol conformance
- Protect against vulnerabilities (OWASP Top 10 API)
- Anti DDoS and bot mitigation
- JSON content/payload inspection



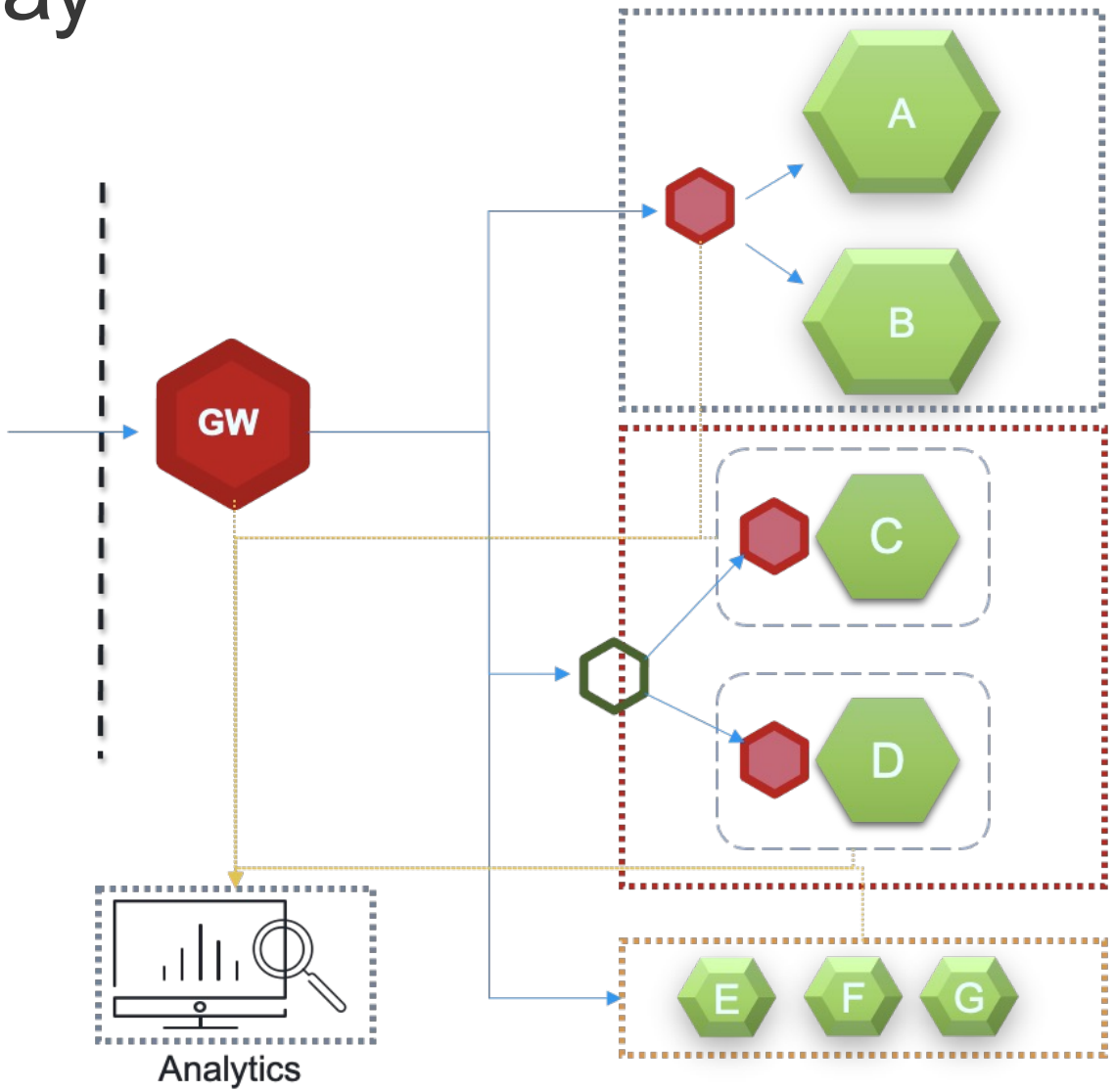
Key Area #2 – API Management

- Versioning
- Publishing
- Schema and definition
- Monitoring and dashboarding
- Onboarding and docs

OpenAPI Specification

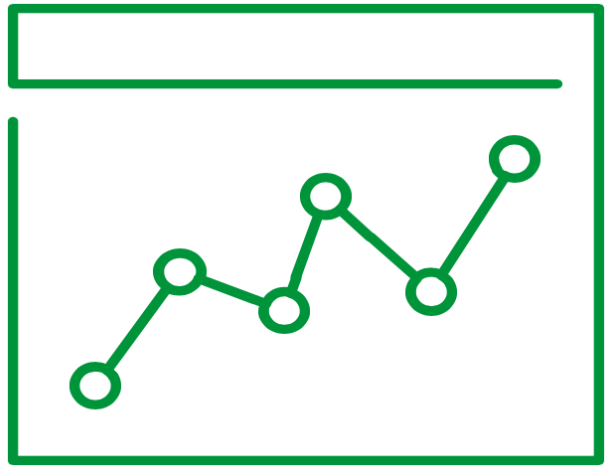
Key Area #3 – API Gateway

- Authentication and authorisation
- Traffic management
- Rate limiting
- Allow list
- Routing

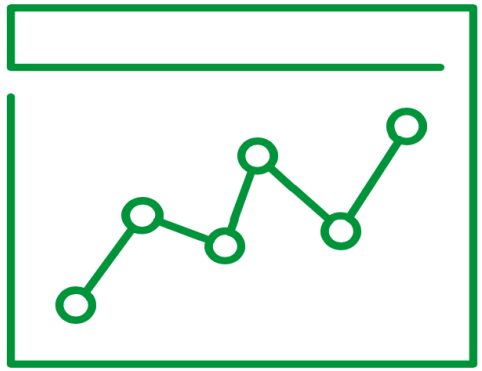


Key Area #4 – API Performance and Availability

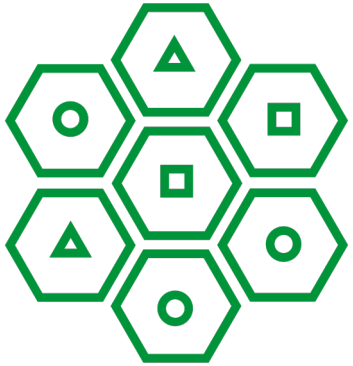
- Decoupled data plane from the control plane
- Enhanced scalability of API gateway instances
- Autoscale data plane based on real-time metrics



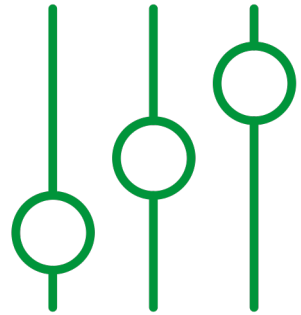
NGINX Is Best for Performance, Microservices, and DevOps



Automate API management with CI/CD integration



Connect microservices API traffic



Improve scale and performance of APIs

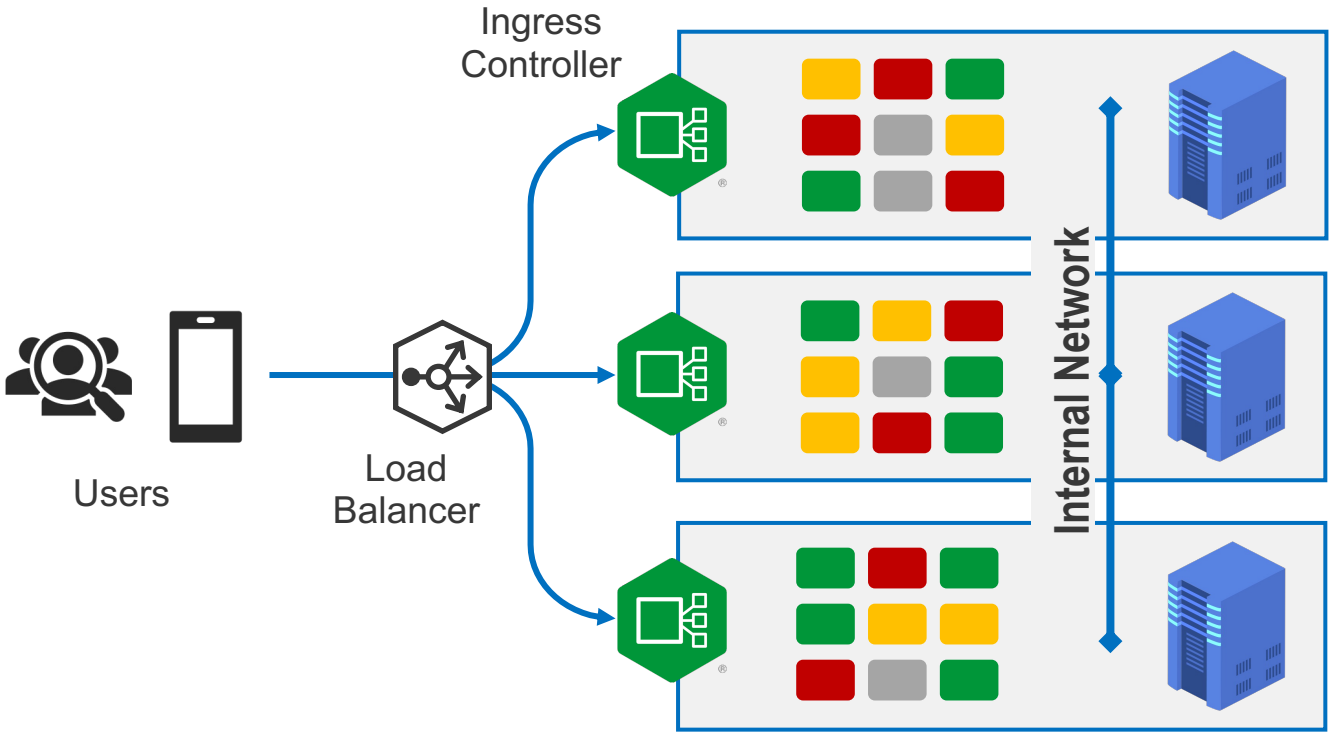
NGINX API Management

API Definition & Publication	Authentication & Authorization	Rate Limiting
Monitor & Analyze Performance	Dashboard	OpenAPI Spec support
Support for DevOps	Security	API Developer Portal

NGINX Ingress Controller

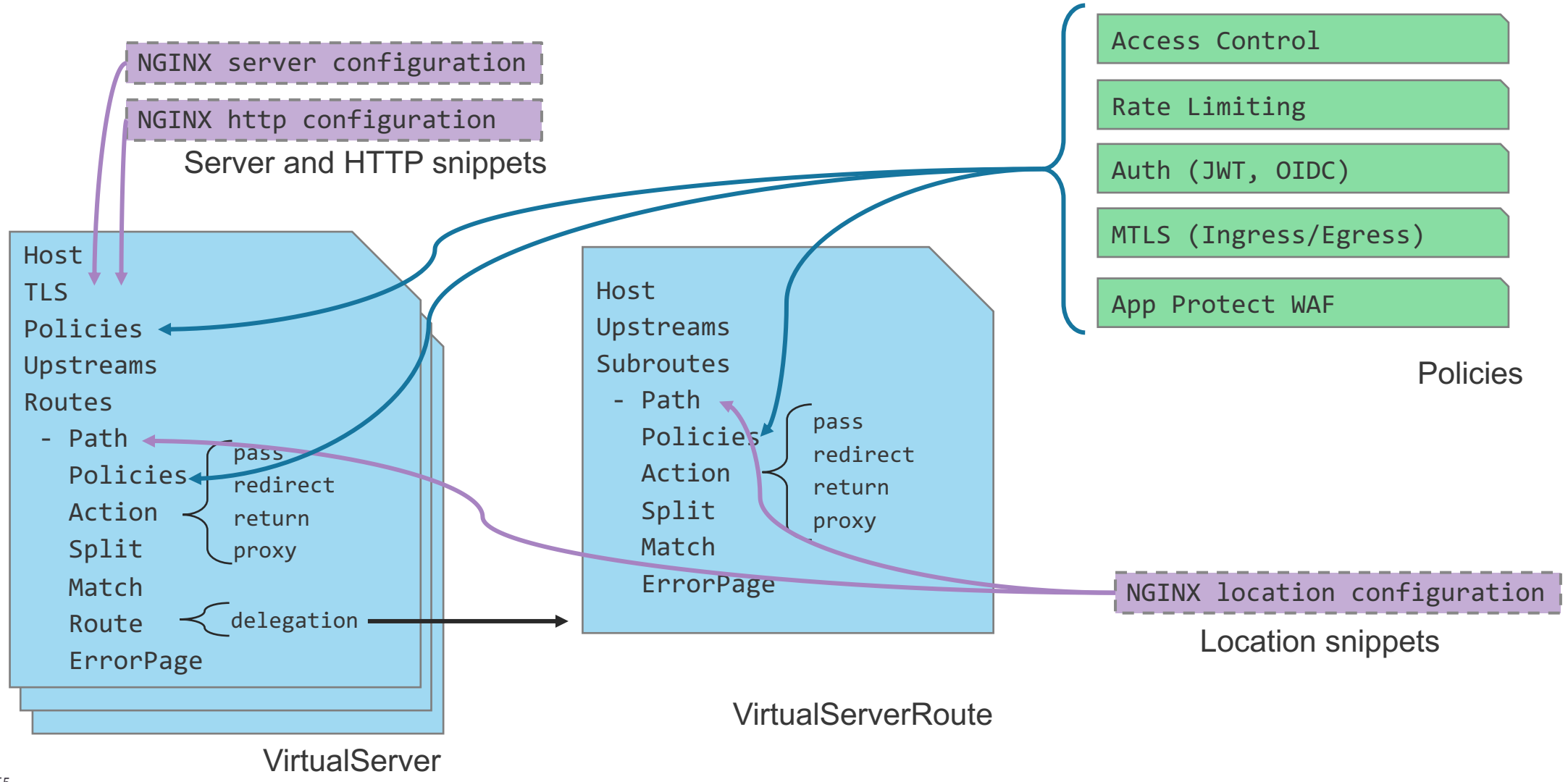
What is an Ingress Controller?

A specialized load balancer for Kubernetes environments:



- Accepts traffic from outside the Kubernetes platform, and load-balances it to pods (containers) running inside the platform
- One single IP address and load balancer for multiple applications, routing is based on URI's (L7 info)
- Monitors the pods running in Kubernetes, and automatically updates the load balancing rules if, for example, pods are added or removed from a service

NGINX Ingress Resources – Rich Capabilities

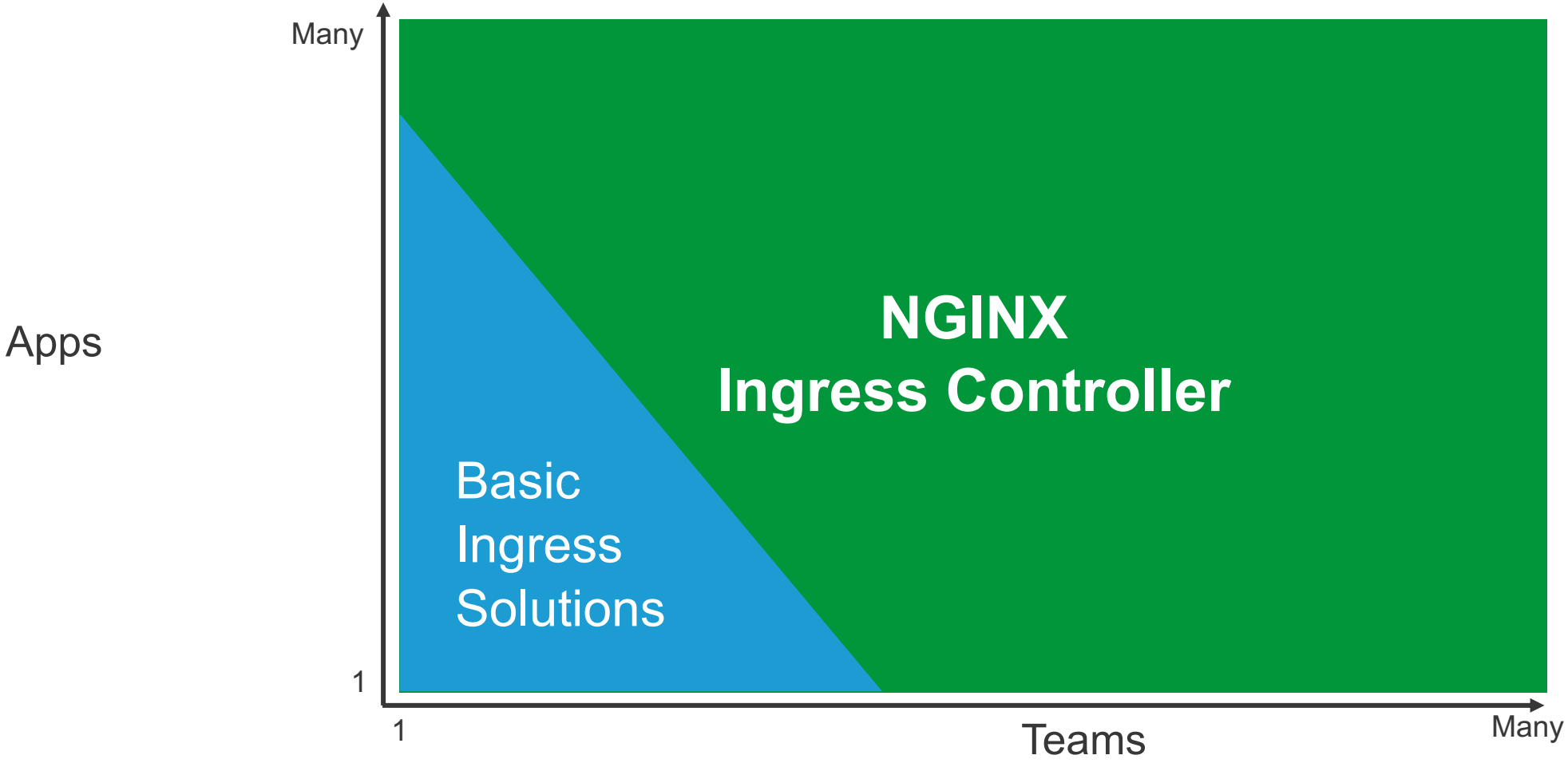


NGINX Ingress Controller - Use Cases

Conditional Routing	→	*Multiple versions, multiple clients*
Split Routing	→	*A|B Testing for safe production deployment*
Error Pages	→	*Implement 'Circuit Breakers' to contain failures*
Rate Limiting	→	*Protect vulnerable apps, limit greedy clients*
Authentication	→	*Offload identity checking from apps and centralize*
Web Application Firewall	→	*Protect from known and unknown vulnerabilities*
NGINX Snippets	→	*"to-the-metal" with NGINX configuration*

Manage Complexity in Production

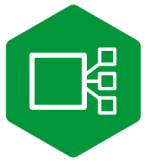
WITH KUBERNETES & NGINX INGRESS CONTROLLER



Why not use the Community version of NGINX Ingress Controller?

WAIT, THERE'S MORE THAN ONE?

Driven by innovation at the expense of feature stability



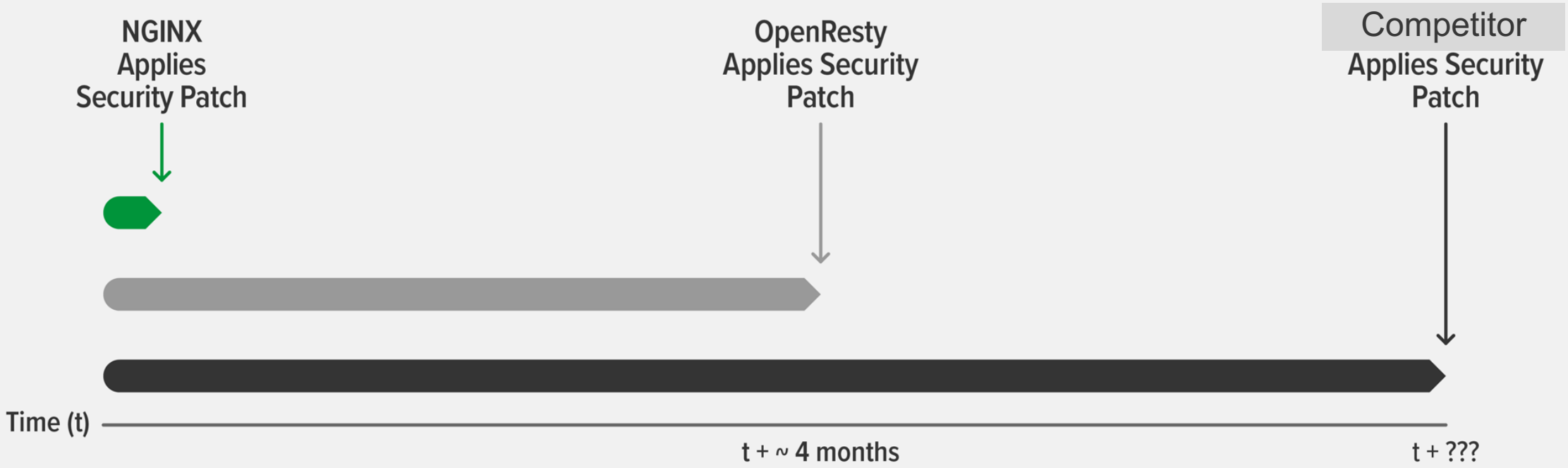
NGINX Ingress Controller®

Driven by enterprise-ready stability without compromising innovation

Footprint	Community: 500MB NGINX Plus: 120MB
Latency	Community: Slowed by timeouts NGINX Plus: Dynamically reconfigures
Timeouts	Community: 8809 NGINX Plus: 0
Security	Community: OpenResty = CVE problems NGINX Plus: Proactive CVE patching, Integrated WAF & service mesh

Delays in CVE patching

UNNECESSARY RISK IN YOUR K8S ENVIRONMENTS



Demo Time – Ingress Controller

Demo Time – Ingress Control