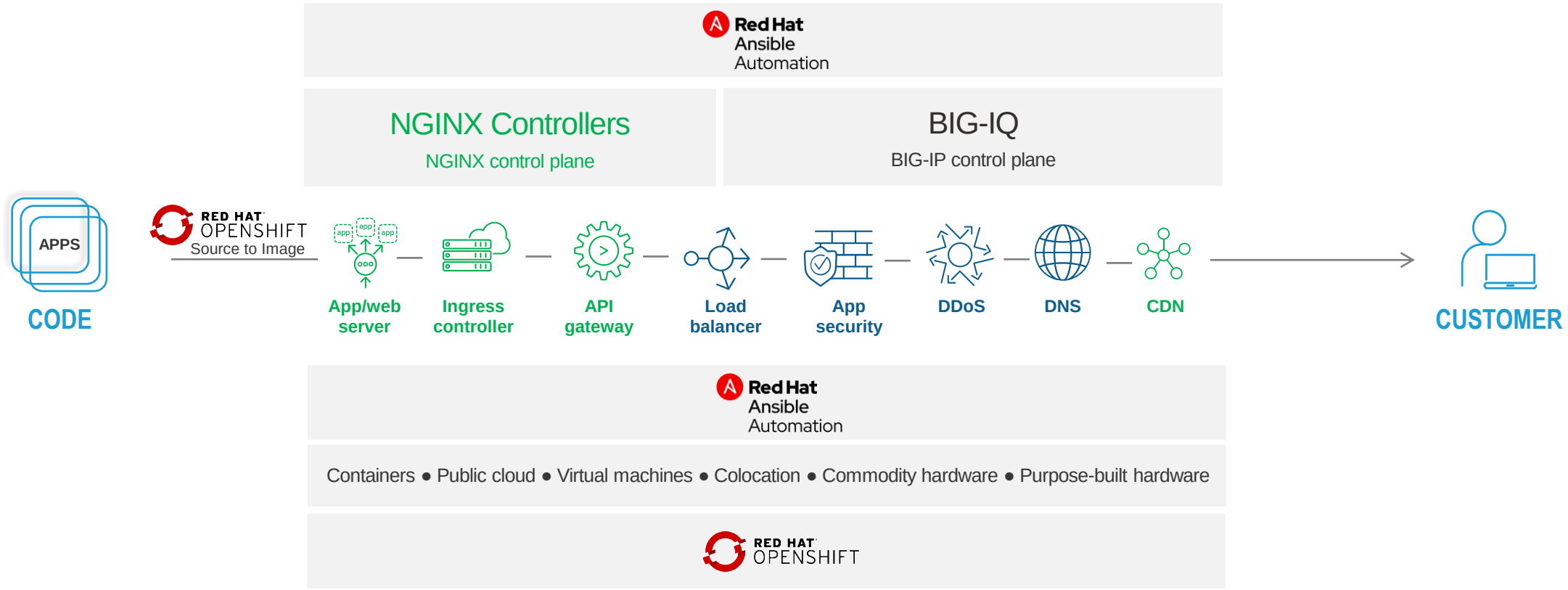
# Migrate, Scale, and Secure Your OpenShift Kubernetes Deployments with F5 and Red Hat

**Martin Petersen**
Solutions Engineer, F5

**Ralf Brünig**
Solutions Engineer, F5

# Ansible – Automated Application Services

## CODE TO CUSTOMER VISION



# BIG-IP and NGINX Plus in OpenShift

## Advanced Application Services with BIG-IP

Control and secure the traffic to the container platform with F5 Container Ingress Services

## Ingress control

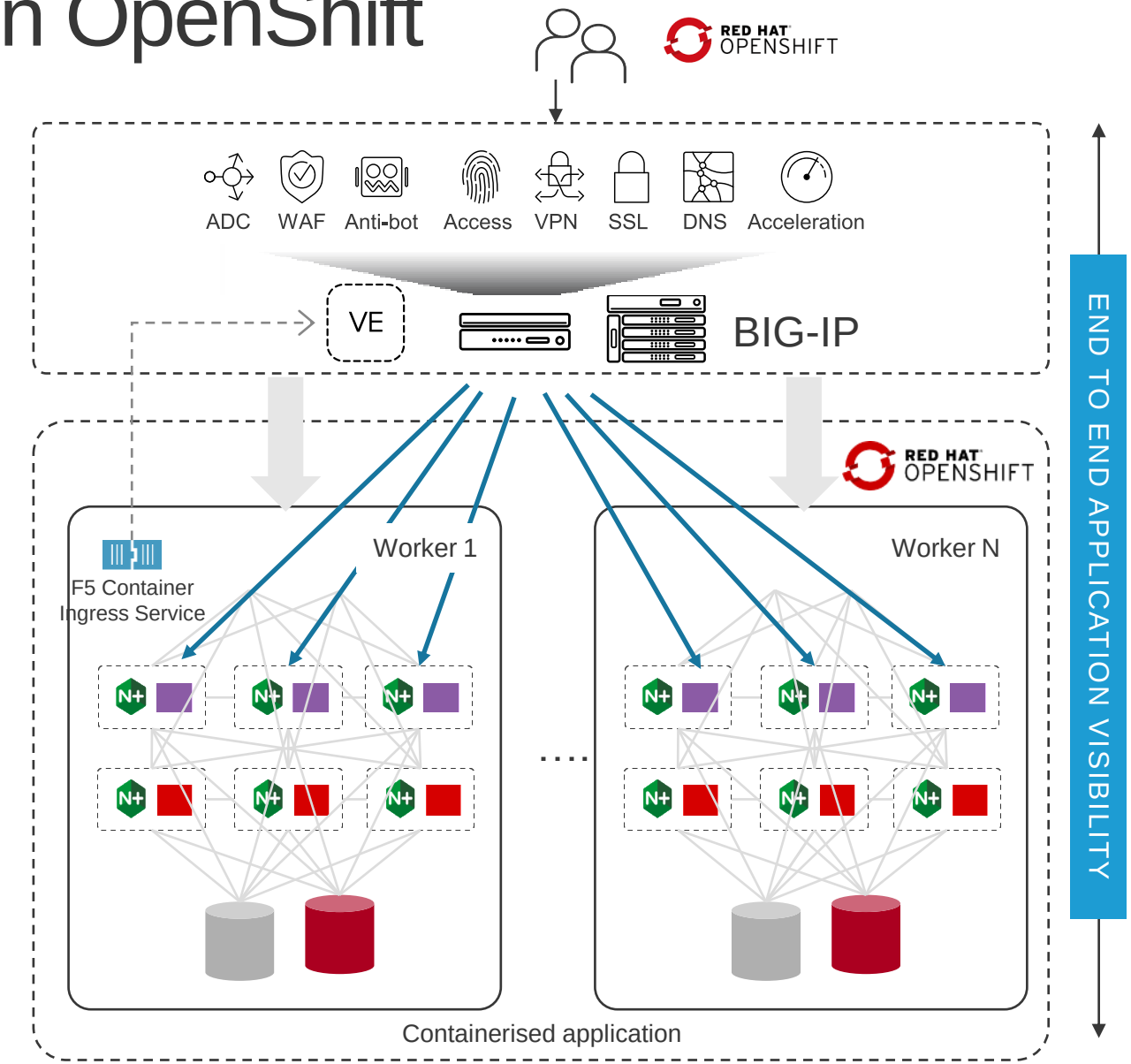
Expose, scale, and secure container-based apps to the world

## Microservices ADC with NGINX Plus

AUTOMATED APP SERVICES FOR INBOUND TRAFFIC

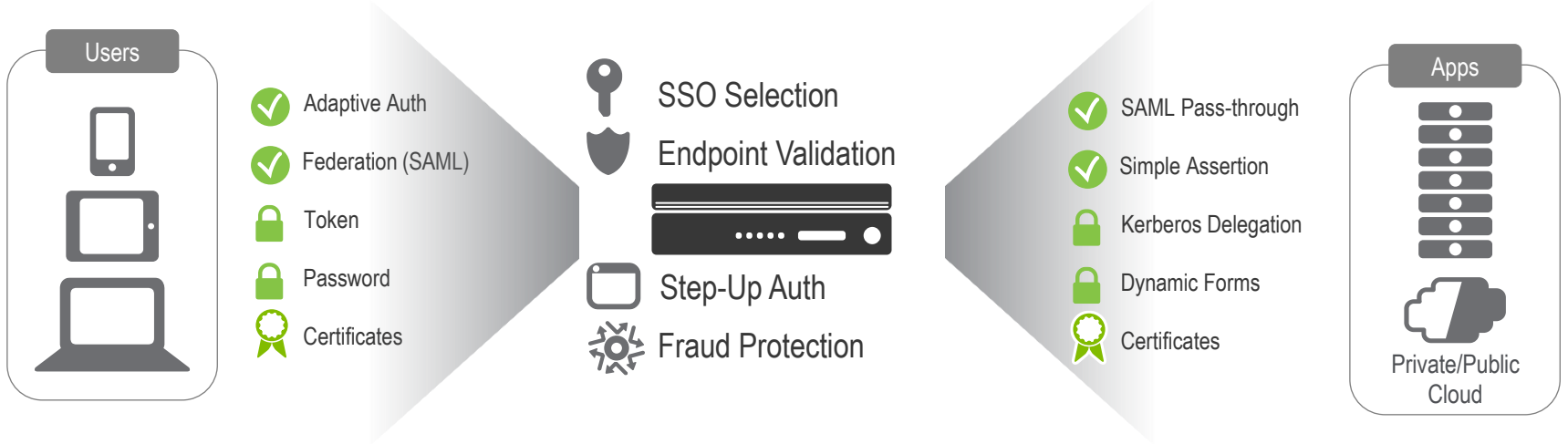
AUTO SERVICE DISCOVERY

MANAGING AND SECURING APPLICATIONS



# Advanced Application Services with BIG-IP

# Adapting access and authentication

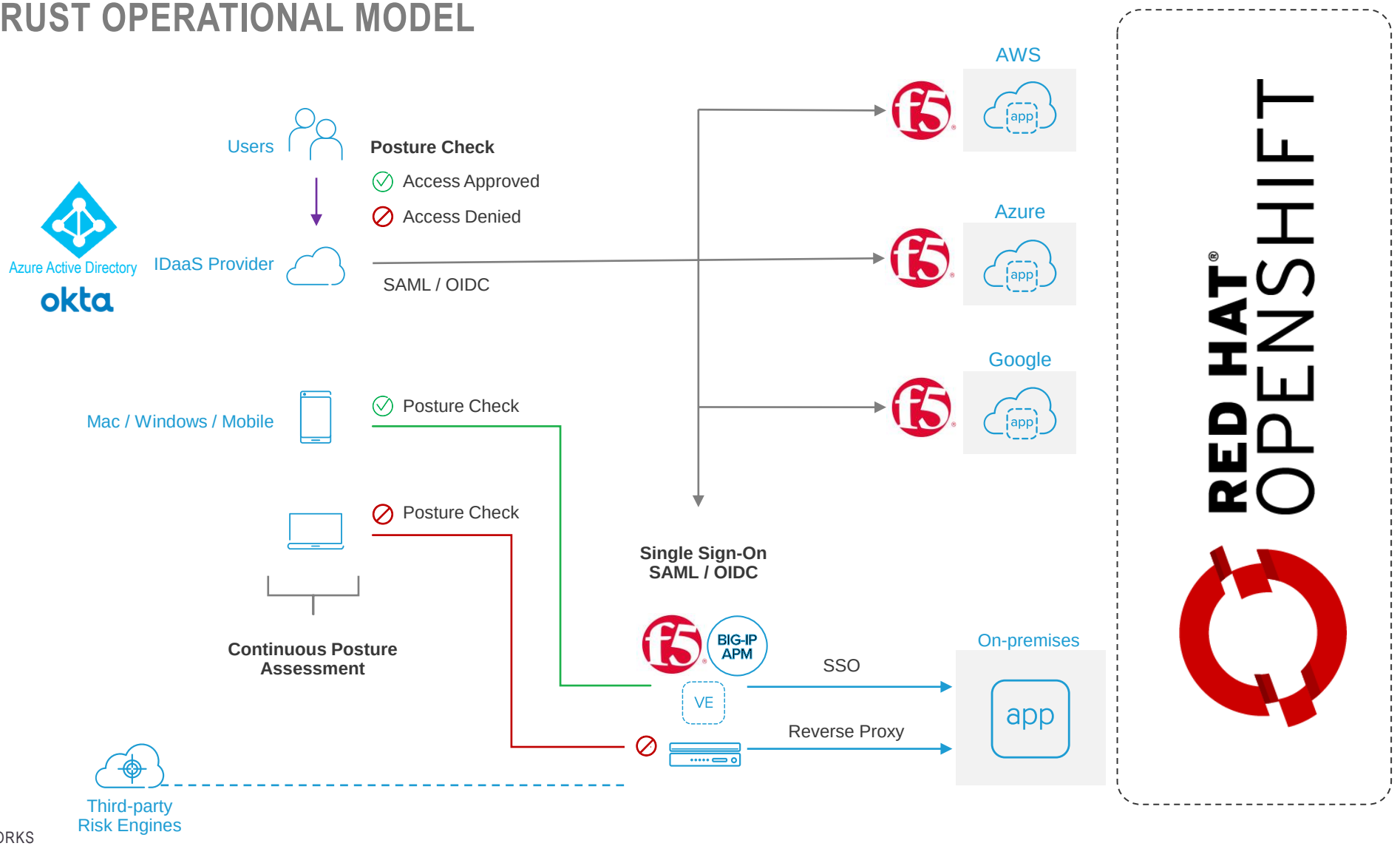



Transform one type of authentication into another so an application may understand and use it without installing additional agents

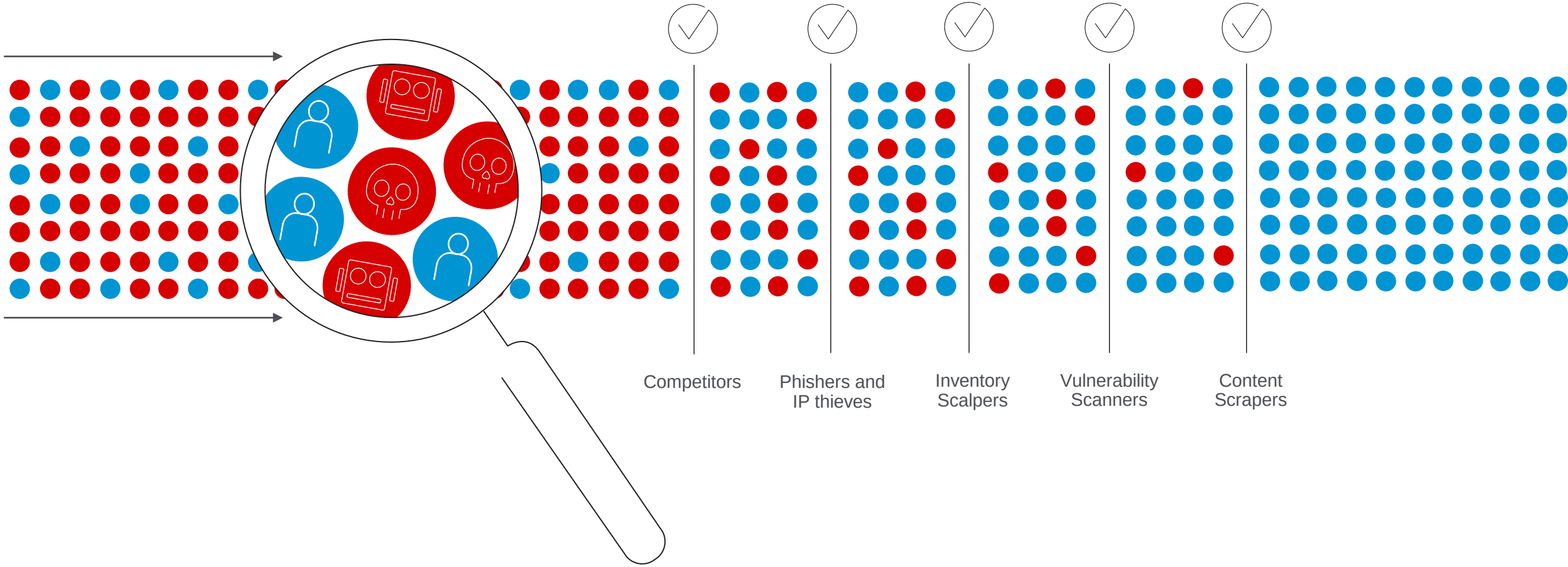
Allow flexible selection of SSO technique appropriate to the application

# BIG-IP APM Identity Aware Proxy architecture

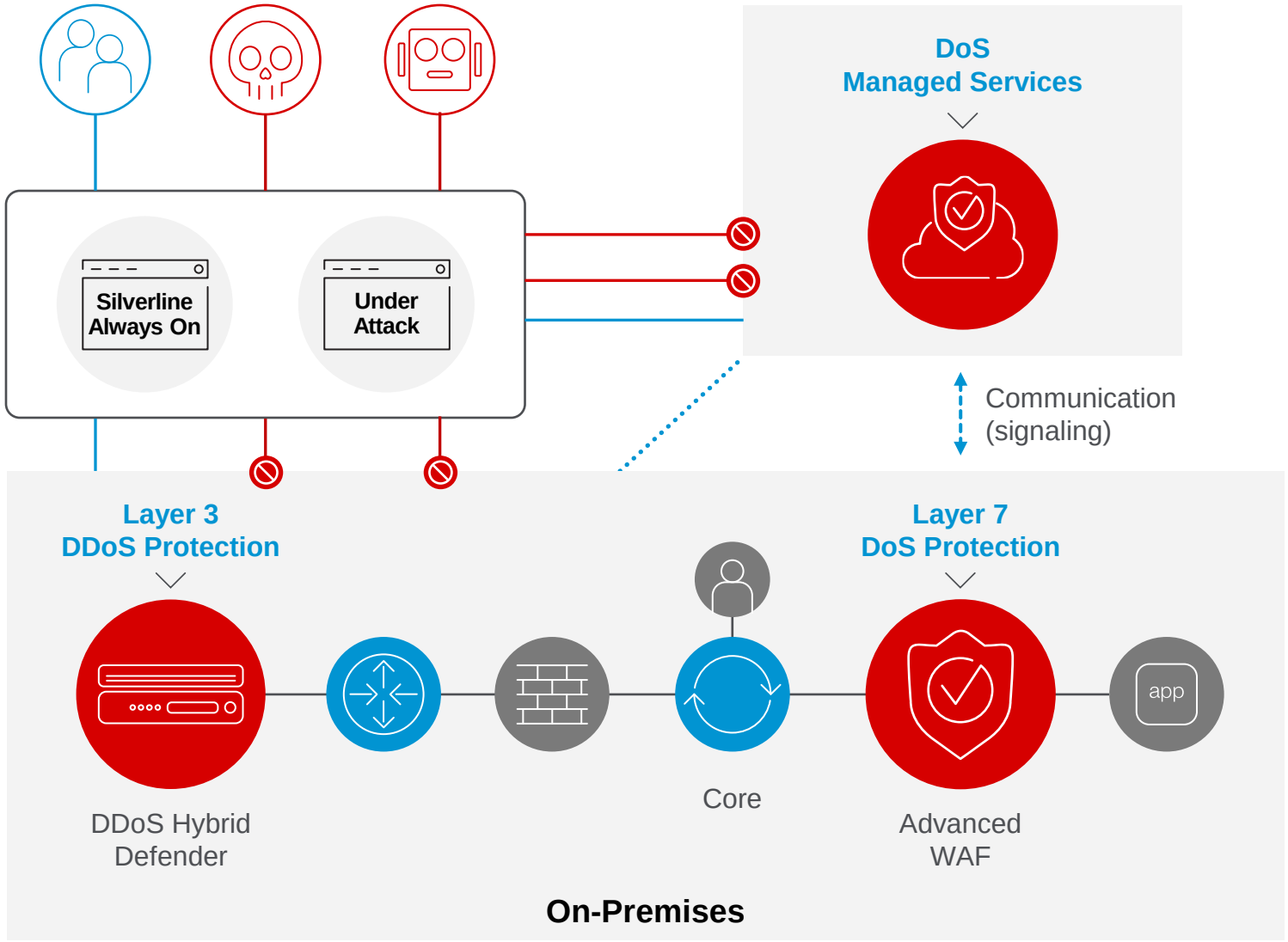
## ZERO TRUST OPERATIONAL MODEL



# Bot Mitigation Can Inform Business Intelligence



# Use Case: DoS Attacks




## Problem

DoS attacks are growing, but your resources are not.

Mitigation time is slow due to manual initiation and difficult policy tuning.

## Solution

Mitigation with layered defense strategy and cloud services.

F5 SOC monitoring with portal.

Protection against all attacks with granular control.

## Benefits

On-premises hardware acts immediately and automatically.

Silverline cloud-based services minimizes risk of larger attacks.

# L7 DoS Mitigation With Behavioral Analytics


## 1 Machine Learning

Learns normal traffic baselines.

## 2 Stress Monitoring

Detects abnormal server stress.

## 3 Dynamic Signatures

Identifies bad traffic and bad actors.

## 4 Attack Mitigation

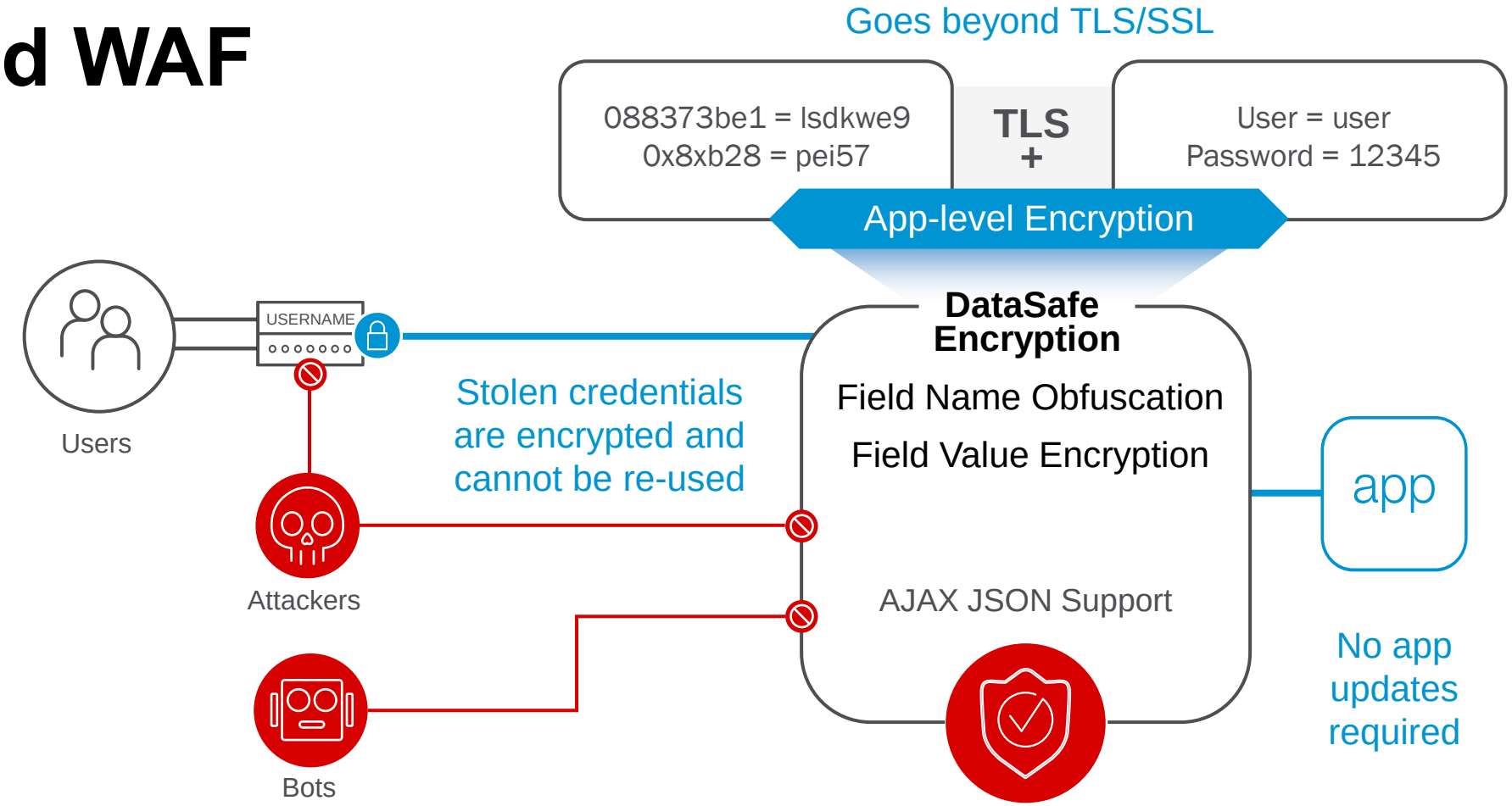
Shuns bad traffic automatically.

# Prevent Data and Credential Theft with F5 Advanced WAF

Application Layer Encryption

Obfuscation and Evasion Detection

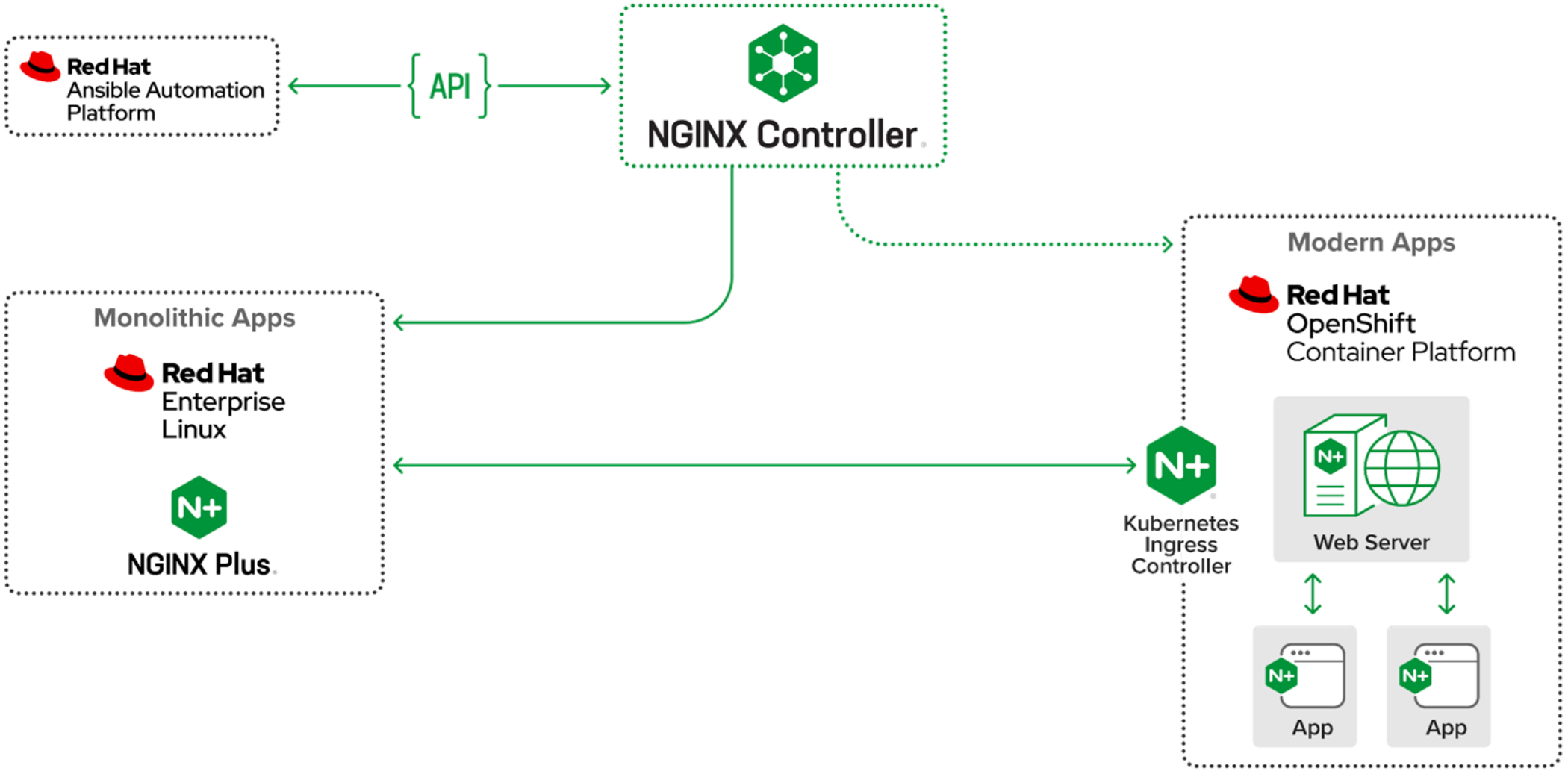
Comprehensive Brute Force Mitigation



# NGINX App Protect

# From Monolithic to Microservices

## NGINX AND RED HAT ARE THERE FOR YOUR JOURNEY



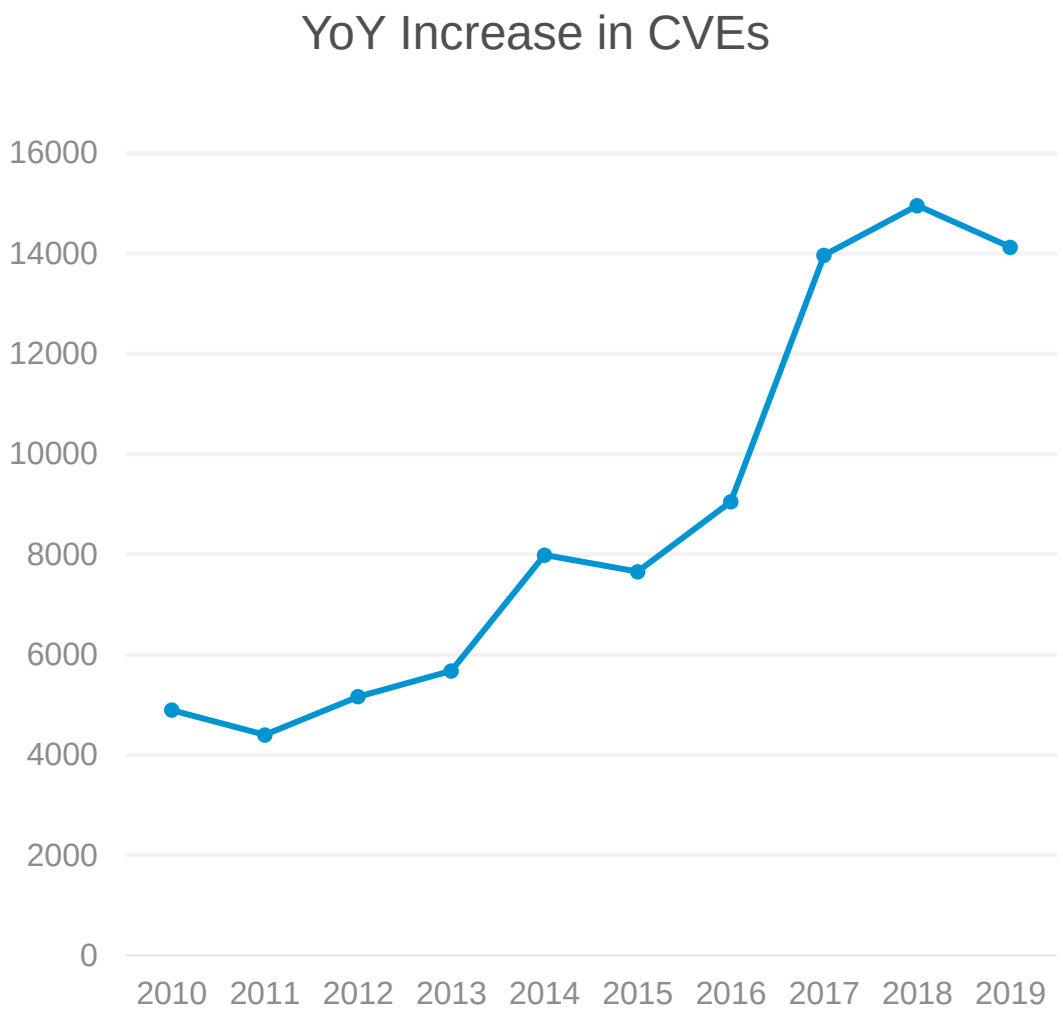
# New vulnerabilities are discovered in all manner of software all the time

They are exploited by both malicious bots and human attackers

Do you know how many affect your application stack(s)?

Can you keep up with the pace of published vulnerabilities?

Do you want to?




Note: Excludes any rejections or disputes.

**REALITY: THE AGILE IMBALANCE**

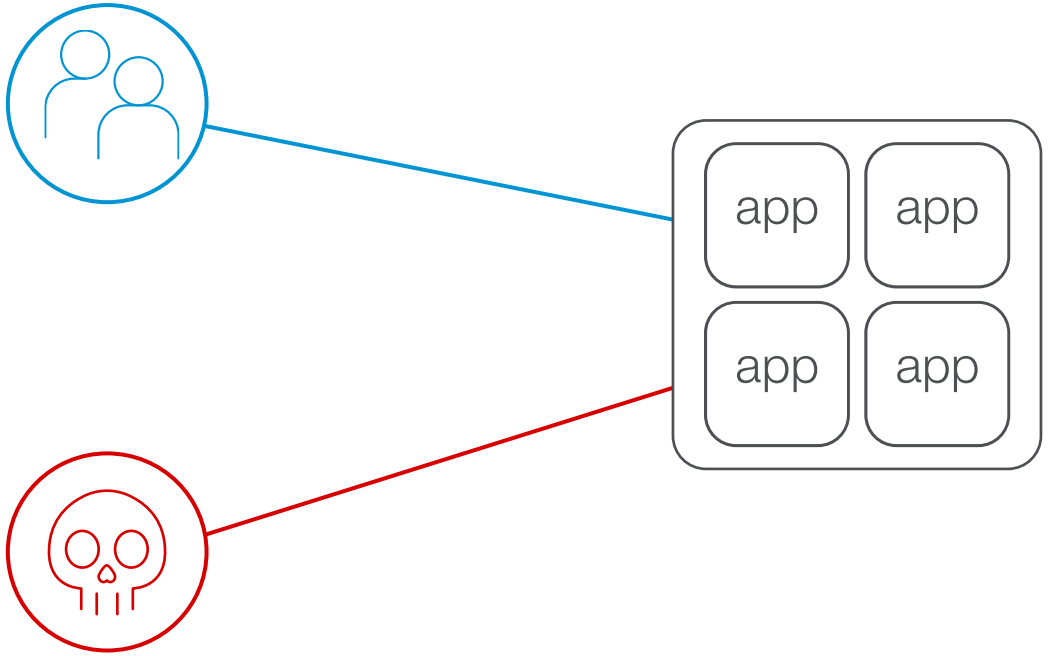
| 100 | 10 | **1** |
|---|---|---|
| Developers | DevOps | **Security** |

# The Pipeline is Built for Speed, Not Security

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

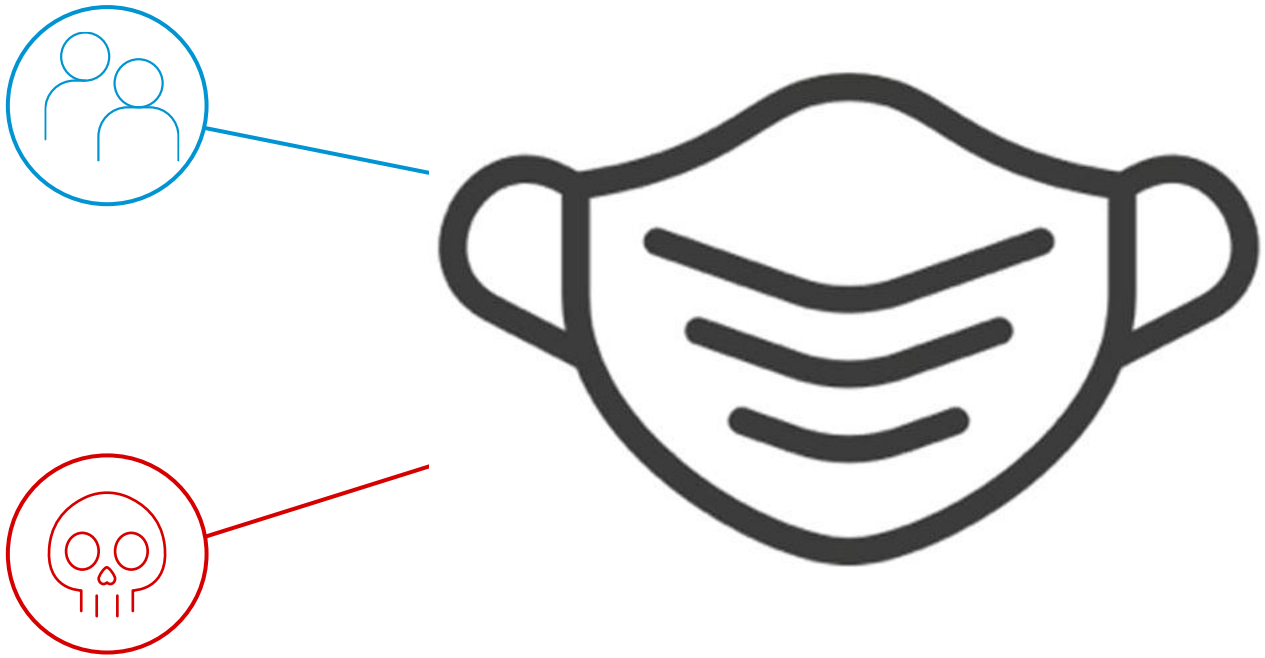
Security control objectives can't be adequately applied and enforced

# How do you protect apps?




- Vulnerabilities
- Active attacks
- Risk and address compliance

# How do you protect apps?

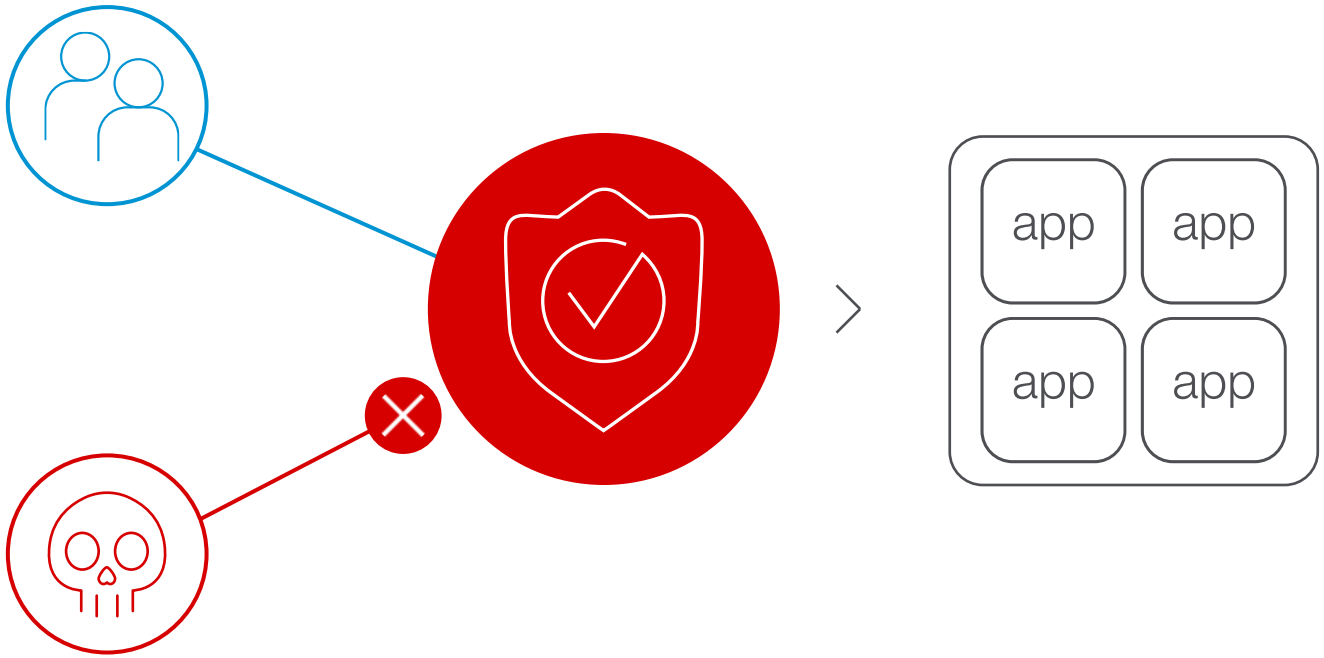


- Vulnerabilities
- Active attacks
- Risk and address compliance

**Web Applications Firewalls (WAF)**

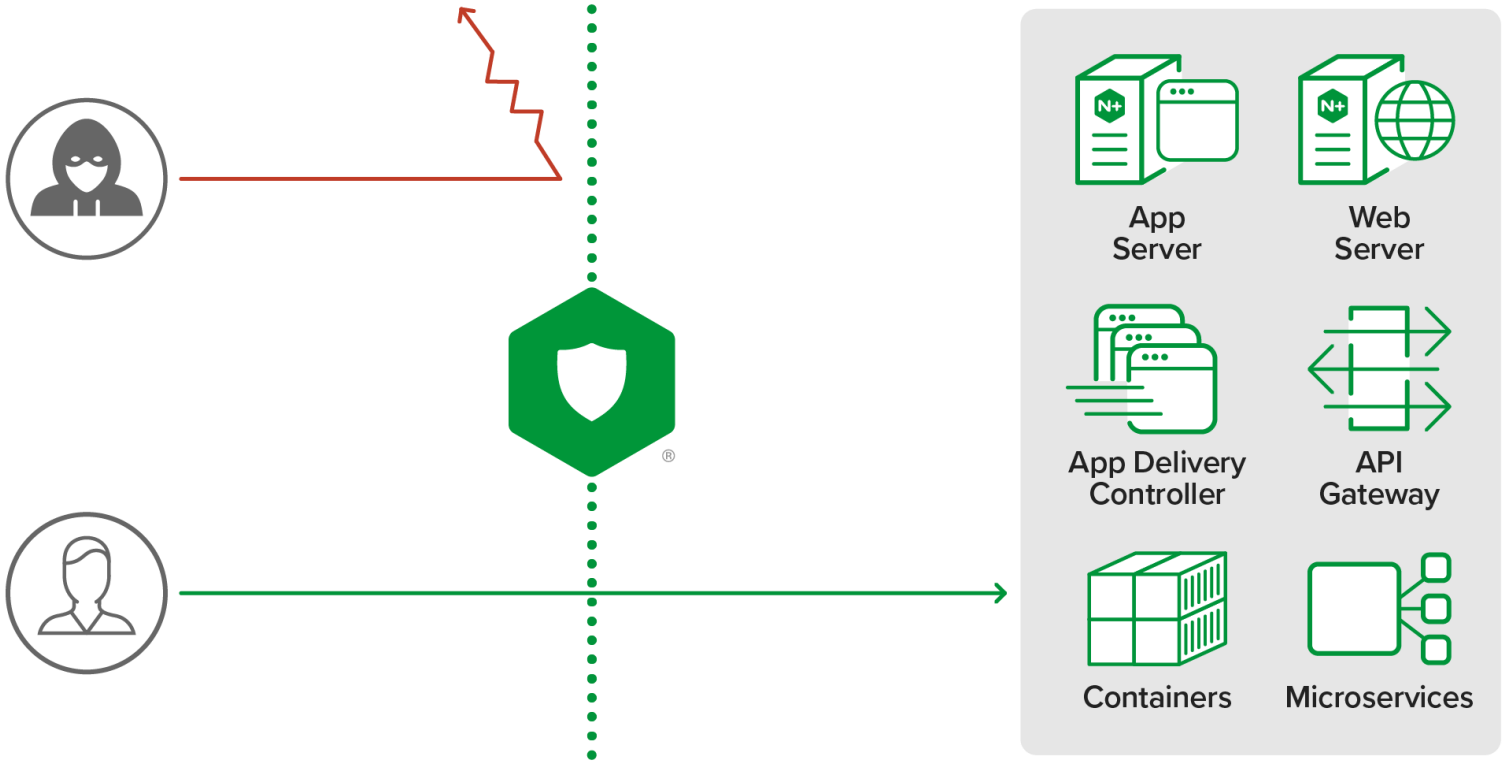
are the fastest and most cost-effective way to address application vulnerabilities

# Web Applications Firewall




- Vulnerabilities
- Active attacks
- Risk and address compliance

# But why NGINX App Protect?




Strong App Security

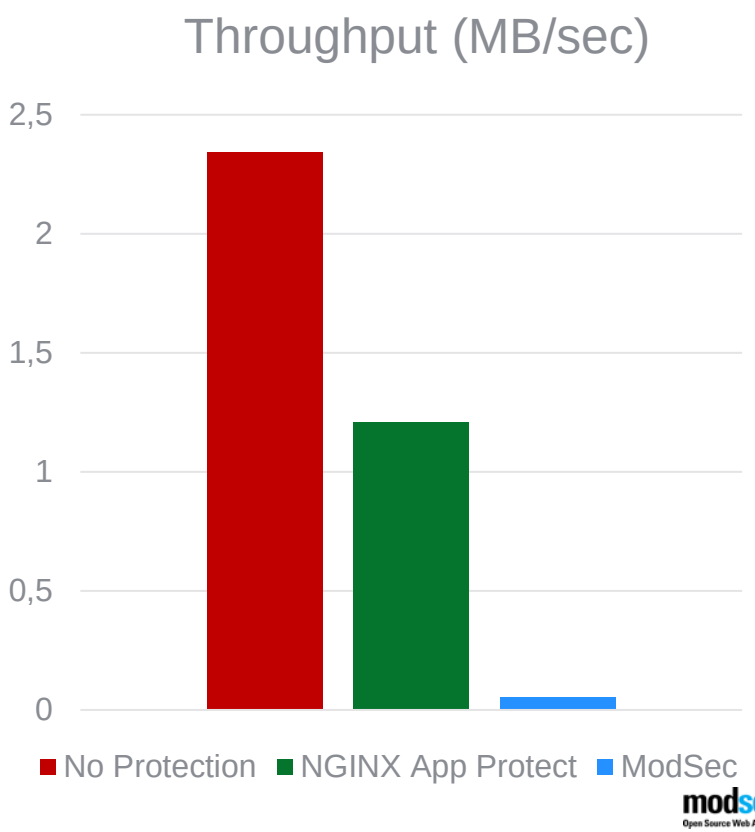
Built for Modern Apps

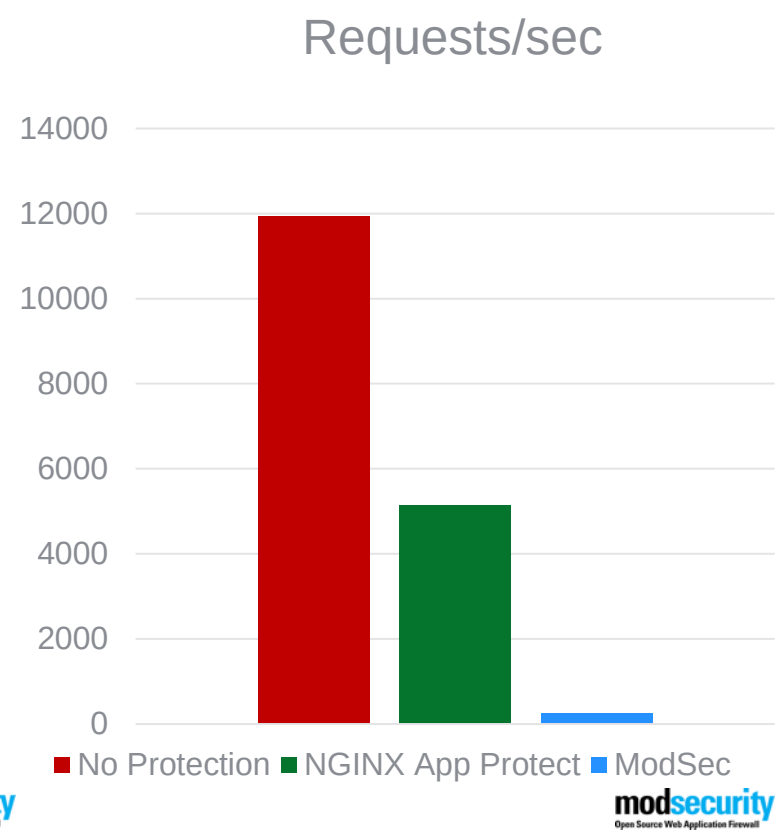
CI/CD Friendly

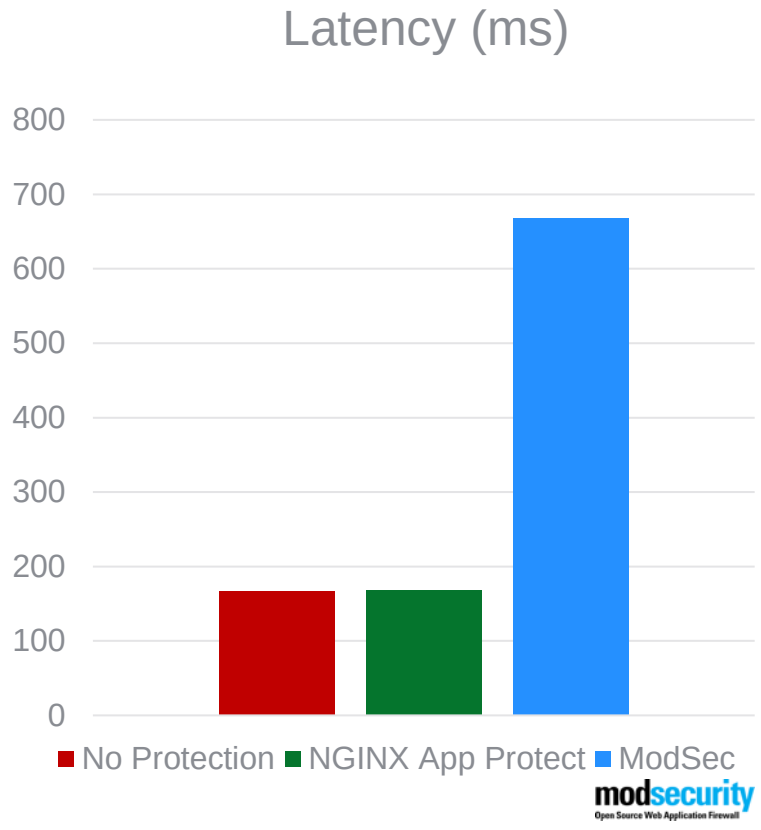
# NGINX App Protect Performance

Comprehensive security policy has no impact on latency, and offers better throughput and requests/second when compared to ModSec

- ModSec Configuration: OWASP Top 10 (enable all CRS 3v rules)
- NGINX App Protect Configuration: OWASP Top 10 (Enable  signatures), Evasion technique, Data Guard, Disallowed file types, HTTP protocol compliance



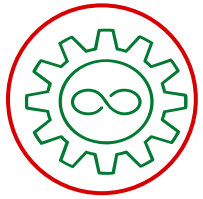



# Enabling *Security as Code*

DEV

SEC



OPS

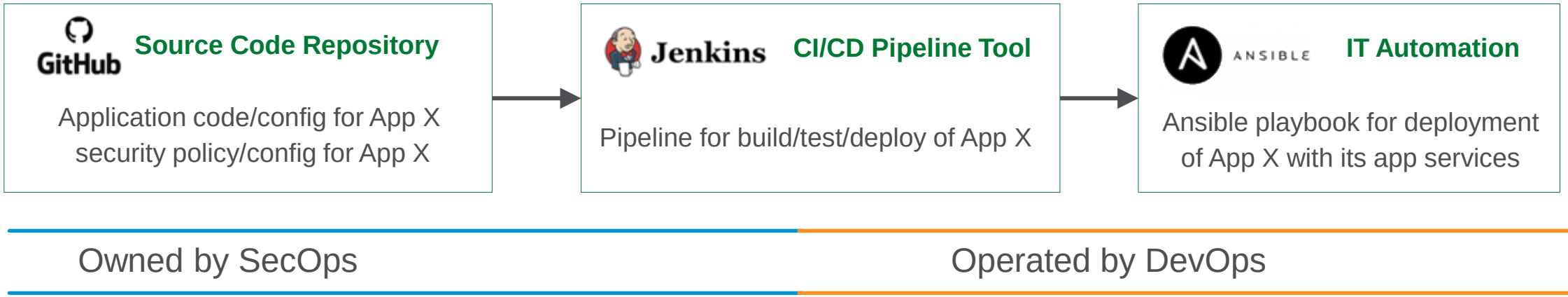
Integration into application security right from the start

Automates security gates to keep the DevOps workflow from slowing down

Enables DevOps to consume SecOps managed policies

# Declarative Policy Helps CI/CD Motion

## INFRASTRUCTURE AND SECURITY AS CODE




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

# F5 and OpenShift

# Certified Operators for both BIG-IP and NGINX Plus


# BIG-IP and NGINX Plus in OpenShift

## Advanced Application Services with BIG-IP

Control and secure the traffic to the container platform with F5 Container Ingress Services

## Ingress control

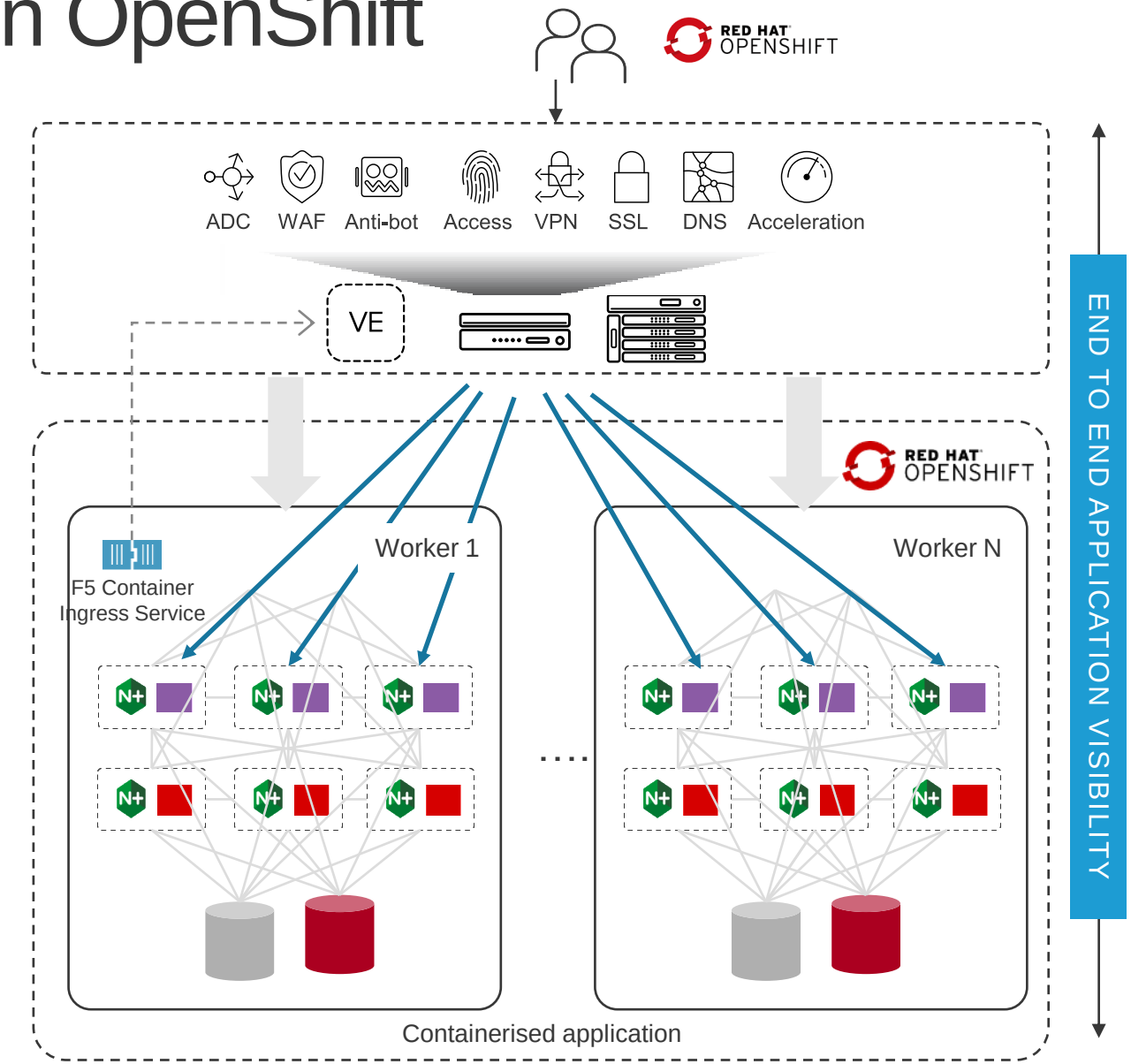
Expose, scale, and secure container-based apps to the world

## Microservices ADC with NGINX Plus

AUTOMATED APP SERVICES FOR INBOUND TRAFFIC

AUTO SERVICE DISCOVERY

MANAGING AND SECURING APPLICATIONS



# F5 Container Integrations: Use Cases

## Frictionless App Services Insertion

### Dynamic App Services for container environments

- Integrate natively with Containers and PaaS for ingress control app performance and security
- Enable self-service for DevOps – deploy app services in seconds within orchestration
- Automated discovery and services insertion – dynamically create, modify, and remove app services

## Align DevOps Velocity with Automated App Services

### Auto-Scale and Secure Cloud Container Apps

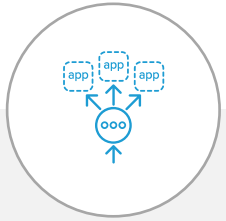
- Spin up/down app delivery services automatically across multi-cloud
- Advanced security protections and mitigate expensive cloud attack traffic
- Flexibility in consuming app services with hourly and subscription Virtual Editions

## Simplify and Centralise Security Services


### Advanced Container App Protection

- Manage app protection with advanced security services
- Automatically create and scale protection by subscribing to container events
- Integrate with vulnerability assessment for patching and gain attack insights from F5 and 3rd party solutions

## Scale Multiple App Versions Simultaneously

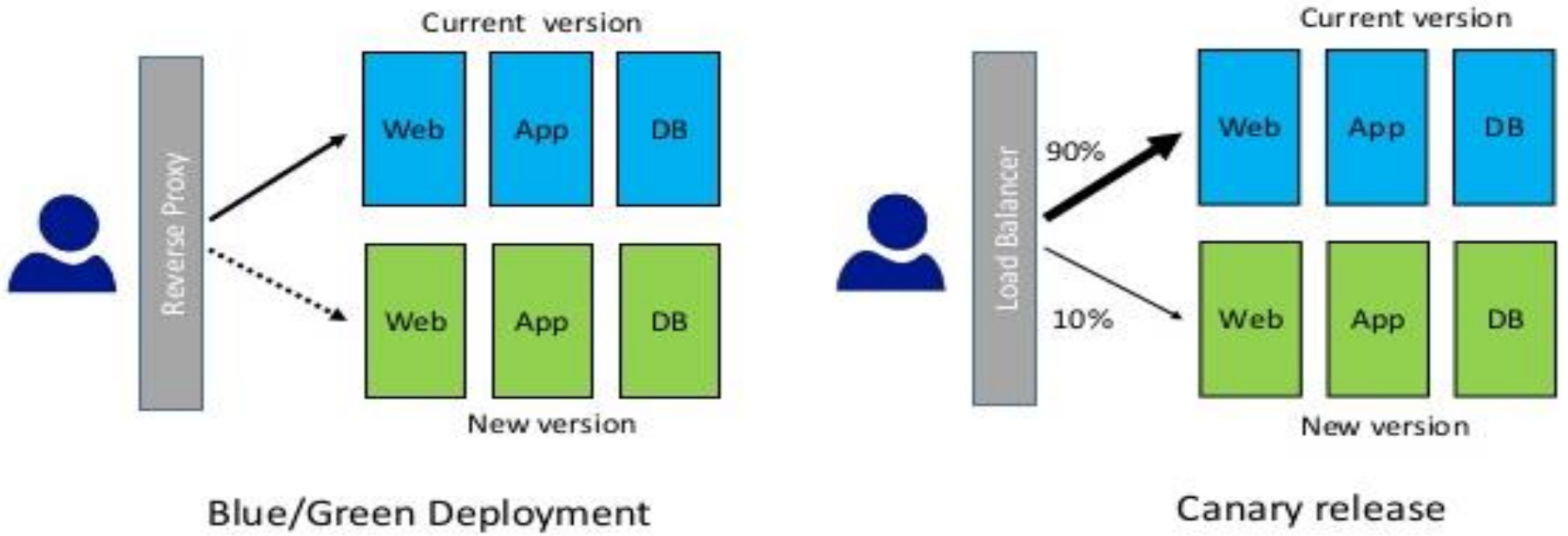



### Streamlined App Migration

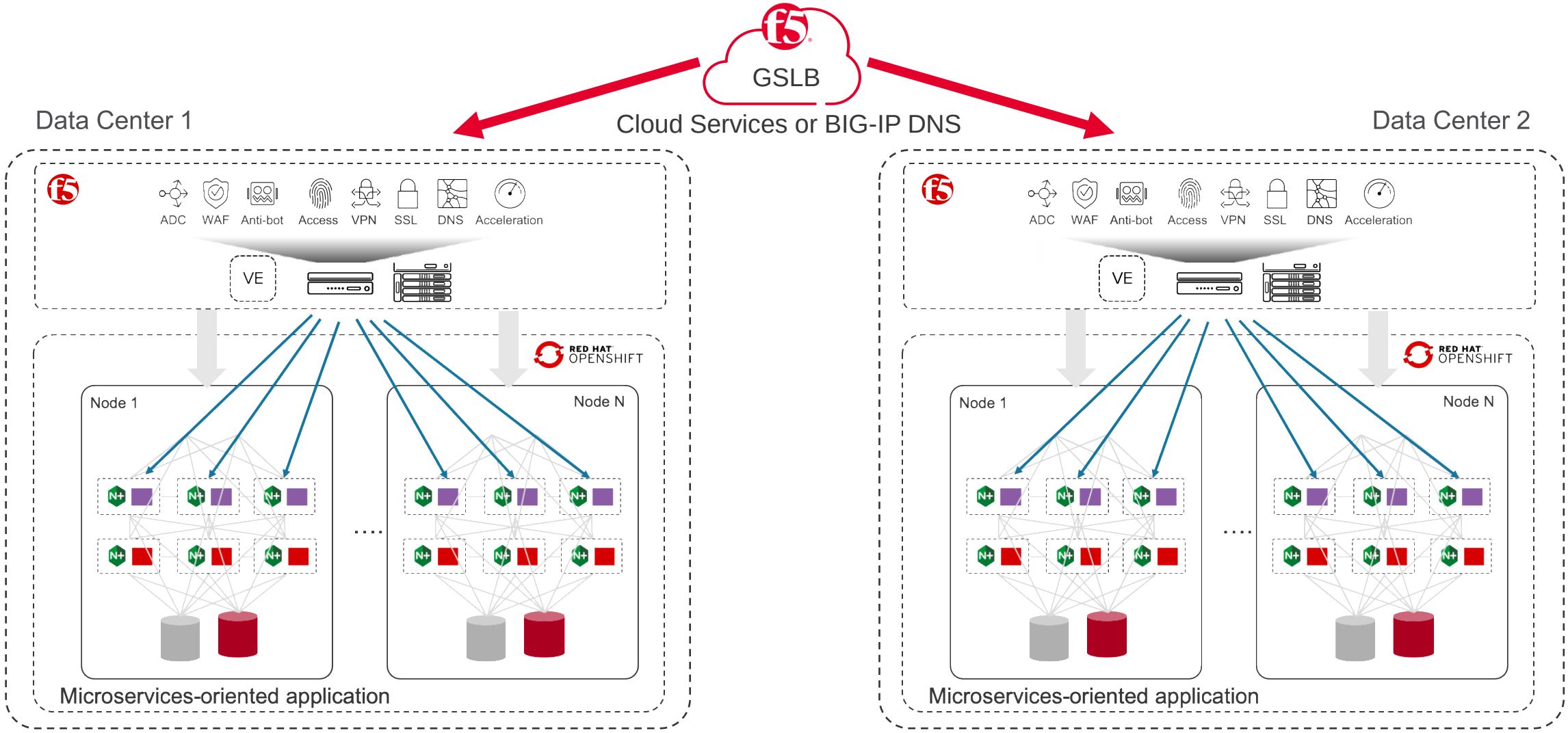
- Leverage A/B testing and Blue/Green traffic management
- Engage many load balancing methods and customise traffic streams
- Protect applications in development and production from malicious attacks and DDoS threats

# Key Use Cases

# Blue-Green vs. Canary Release Methodology



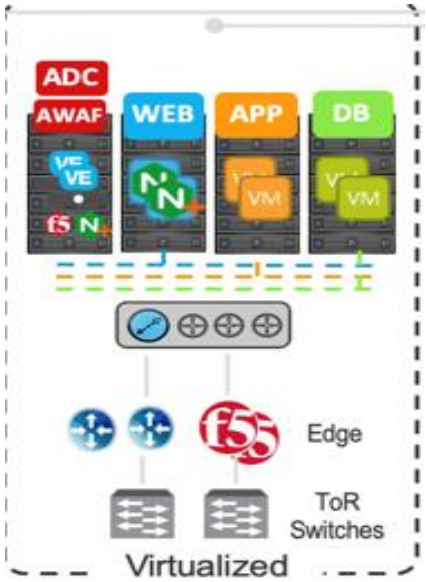
# Resiliency Architecture for Multi-Cluster, Multi-Site Apps



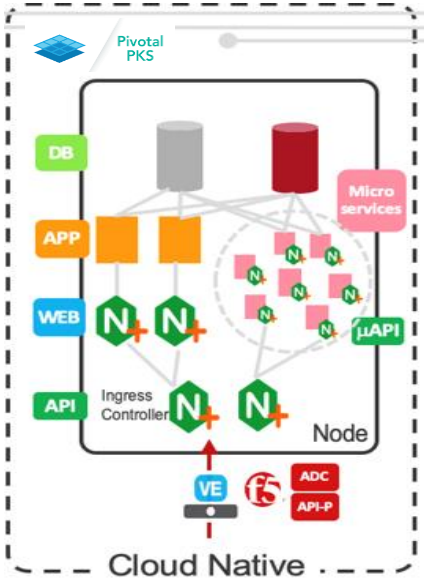
# Multi-Cloud App/Cluster Migration Resiliency

## F5 DNS LOAD BALANCING CLOUD SERVICES

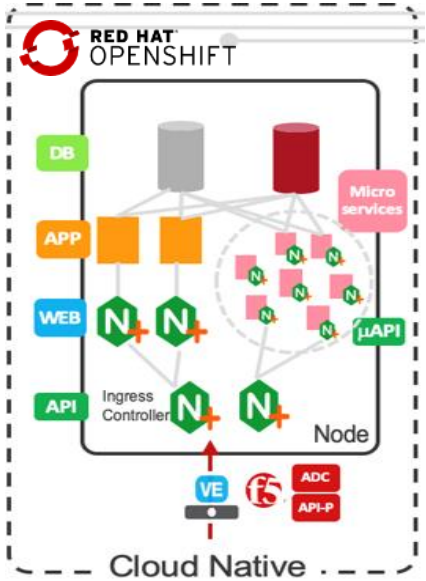
Legacy Application



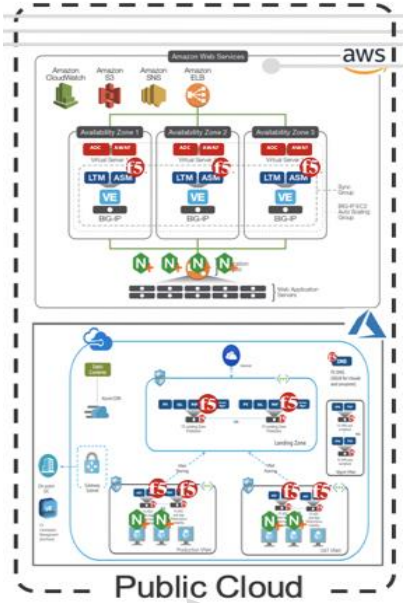

Transformed Application



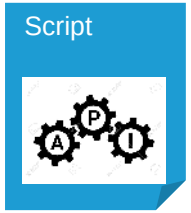

Platform Migration

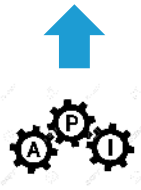


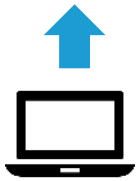

Lift and Shift to Cloud




BIG-IP Intelligent Blue-Green Deployment (DNS)



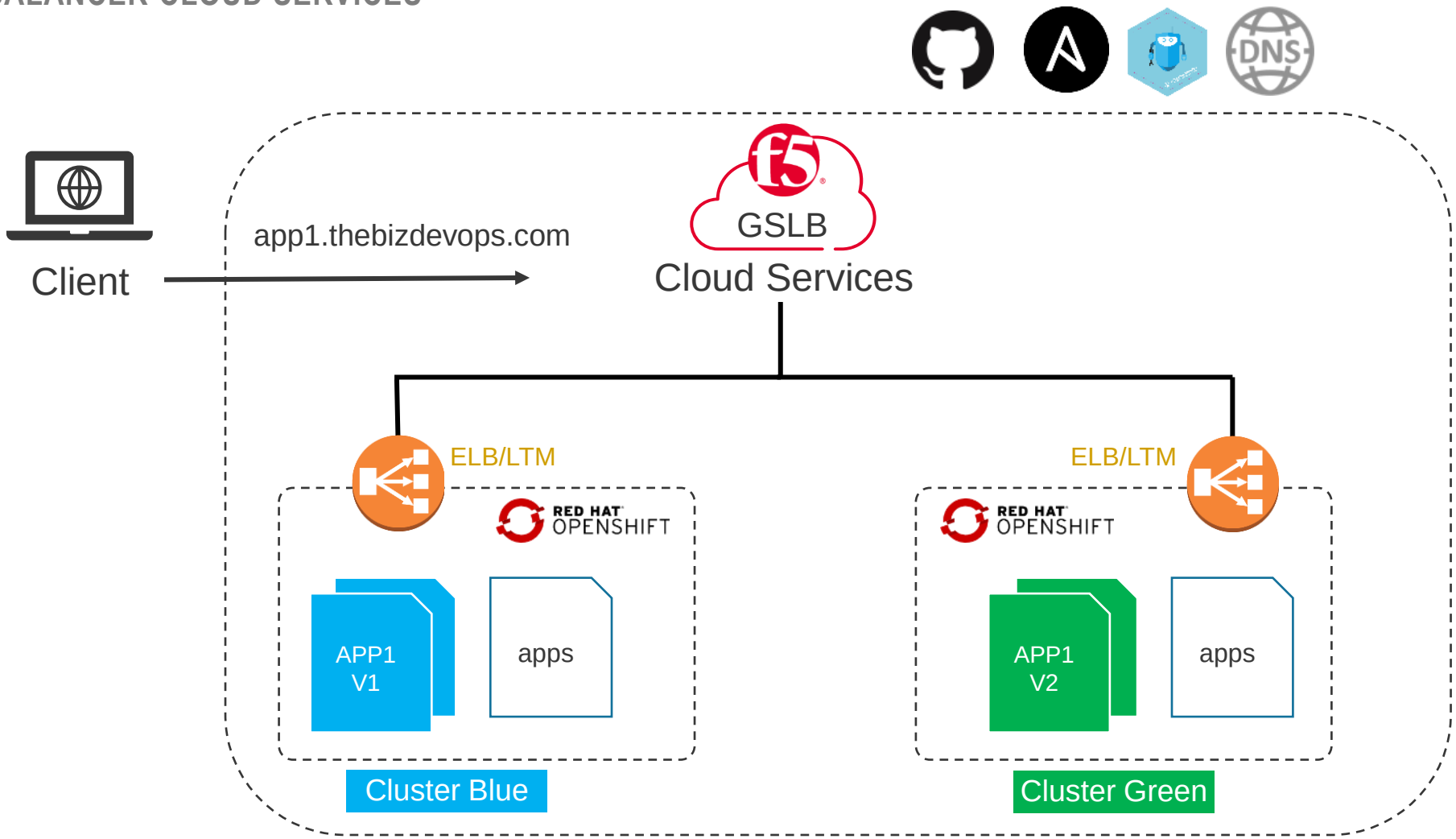







# Blue-Green Efficiencies

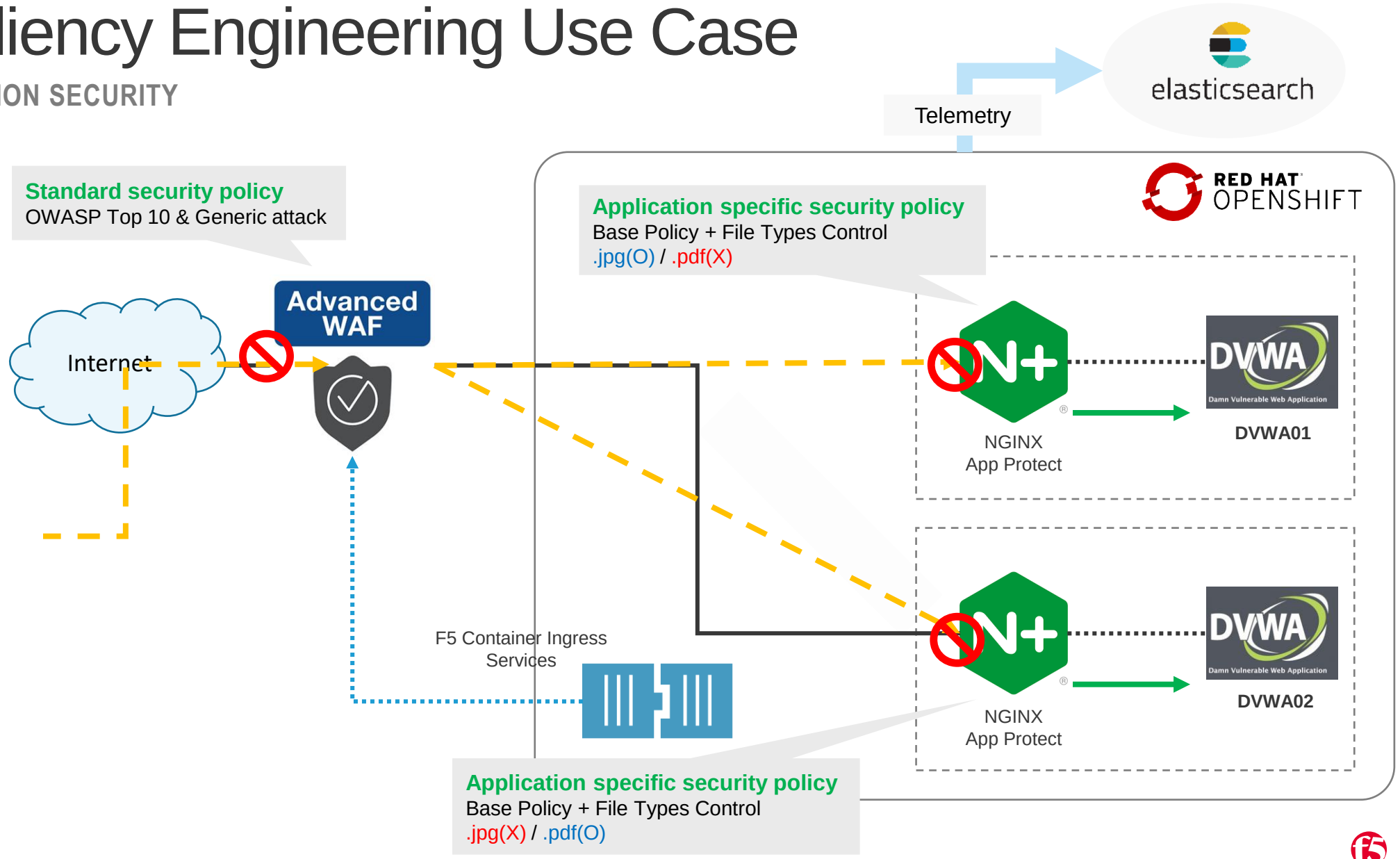
## F5 DNS LOAD BALANCER CLOUD SERVICES



# Site Resiliency Engineering Use Case

## LAYERED APPLICATION SECURITY

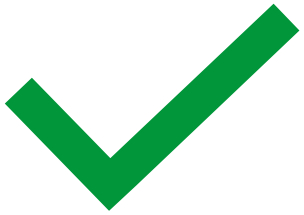
- *Command Injection*
- *SQL Injection*
- *Cross Site Scripting*
- *Server Side Request Forgery*



# Summary and Key Takeaways

# Key Takeaways

Scale and Secure Your Container Deployments with F5 and Red Hat



Provide Site Resiliency Aligned with Agile Development Best Practices

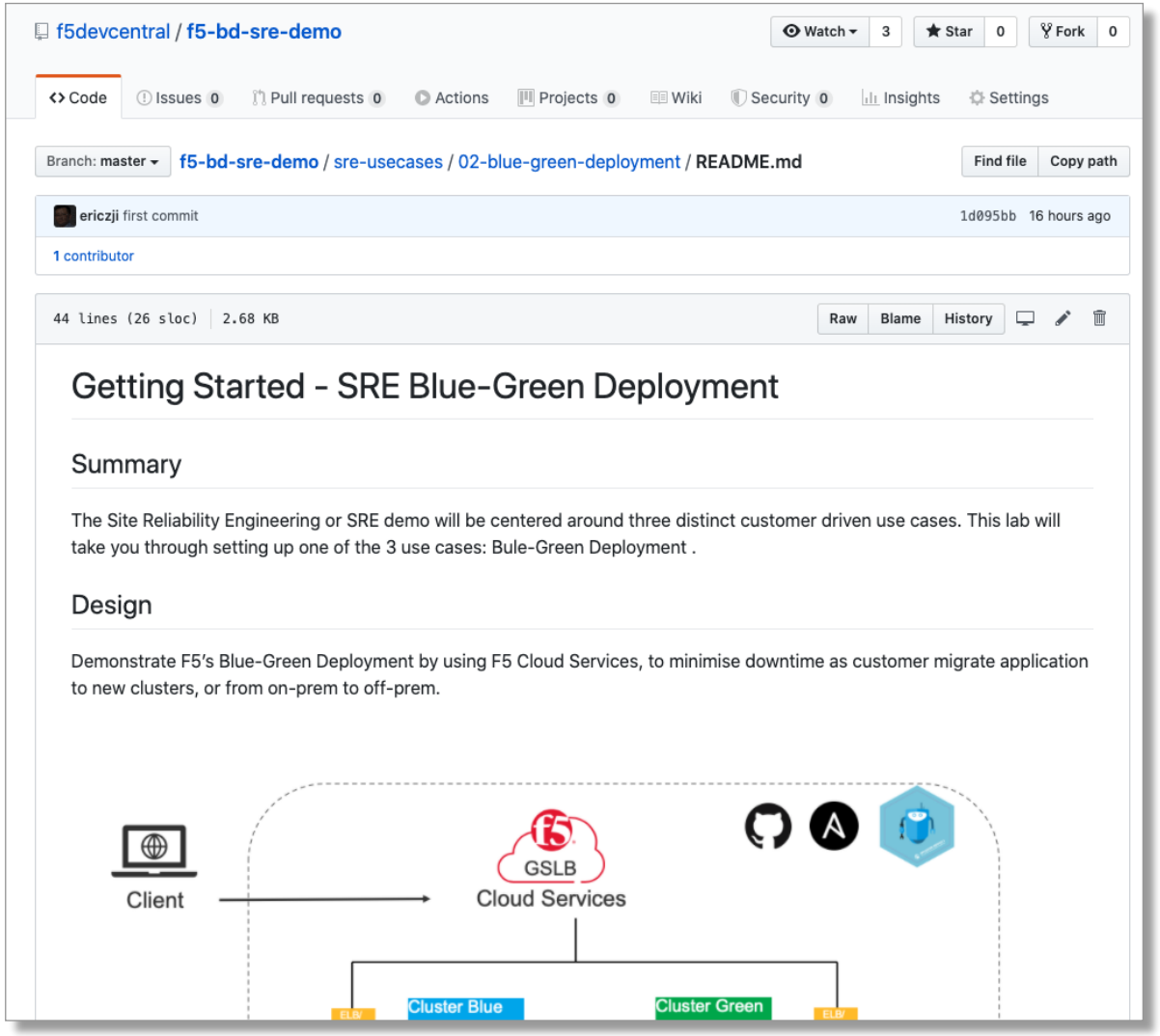
Enable Best-in-Class ADC with Leading Container Platform

# Resources

- SRE Demo GitHub
  https://github.com/f5devcentral/f5-bd-sre-demo

- GSLB Tool
  https://github.com/f5devcentral/f5-bd-gslb-tool

- About F5 & Red Hat
  https://www.f5.com/redhat



# DEMO