September 27, 2022

SLEDFest

Enterprise Application Strategy

PRESENTED BY:

Paul Simmons - Account Manager, Public Sector

Agenda

- What is an Enterprise Application Strategy?

- What is important?
  - Immutability
  - Ephemerality
  - Repeatability
  - Portability
  - Scalability

- Where do I think we are going:
  - SaaS
  - Cloud – All of the clouds
  - On Premises – k8s

- Where does NGINX/F5 Fit in an Enterprise Application Security Strategy?

What is an Enterprise Application Strategy?

It is holistic vision that drives architectures, technology adoption, talent acquisition and security to align with business objectives.

- Talent acquisition
- Adoption of Automation
- Organization structures
- Security Architecture
- Hosting Platforms
- Hosting Locations
- Acquisition Strategies
- Business Objectives
- IT Governance
- Data Management
- Regulatory Compliance
- Accreditation
- Monitoring
- Visibility

What is Important?

Let's talk about the 5 Commandments

1. Thou Shalt Be Immutable
2. Thou Shalt Be Ephemeral
3. Thou Shalt Be Repeatable
4. Thou Shalt Be Portable
5. Thou Shalt Be Scalable

Immutability

Immutable: Unchanging over time, or unable to be changed.

In IT – Unchanging after deployment into production.

Examples:

VDI
Kubernetes
Cloud - When done correctly

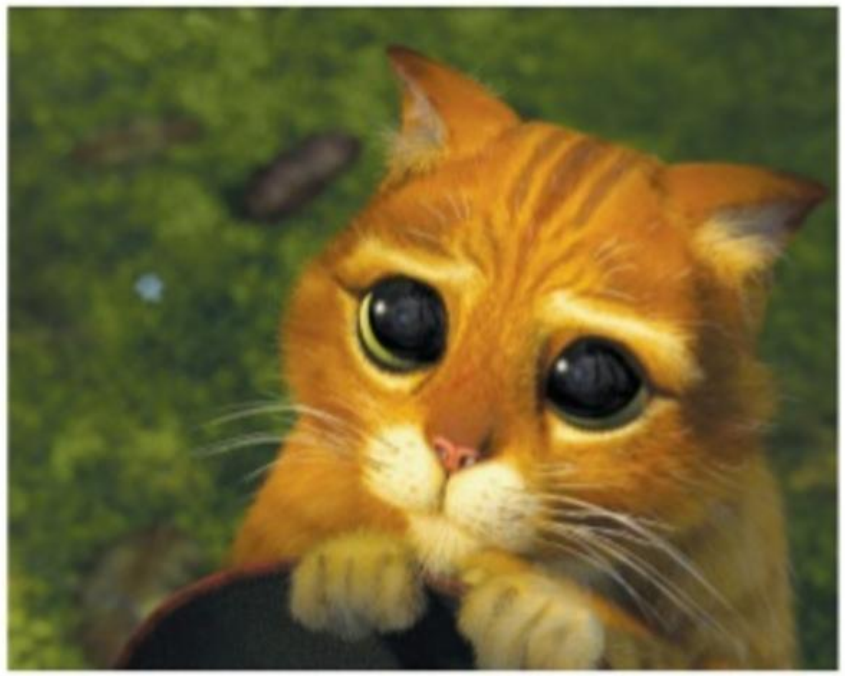
Ephemerality

Ephemerality: (from the Greek word ἐφήμερος, meaning 'lasting only one day') is the concept of things being transitory, existing only briefly.

In IT: Cattle not Pets

Examples:

VDI
Kubernetes
UDF Labs

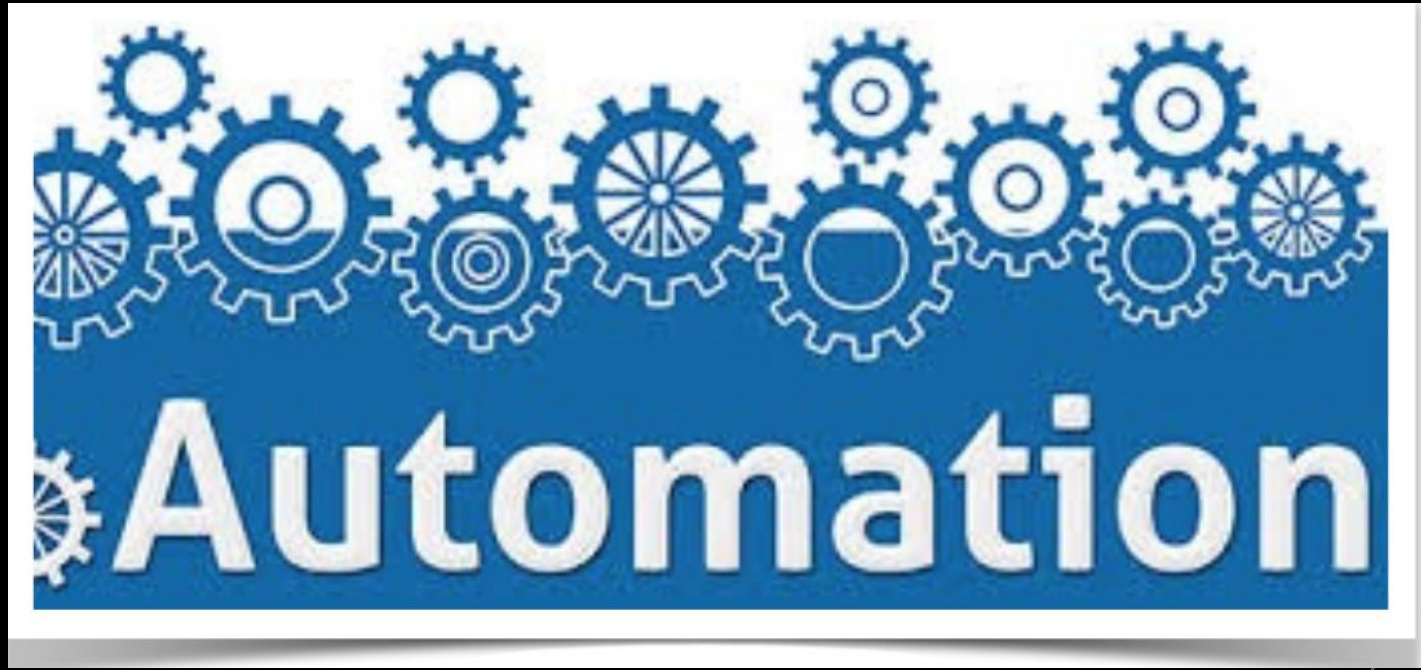


Repeatability

Repeatability: is the closeness of the agreement between the results of successive measurements of the same measure, when carried out under the same conditions of measurement.

In IT: Can I do the same thing over and over and get the same results?

Examples:
Ansible
Terraform
etc



Portability

Portability: the ability of software to be transferred from one machine or system to another.

In IT: Can it run in all the clouds and on Prem or even tactically.

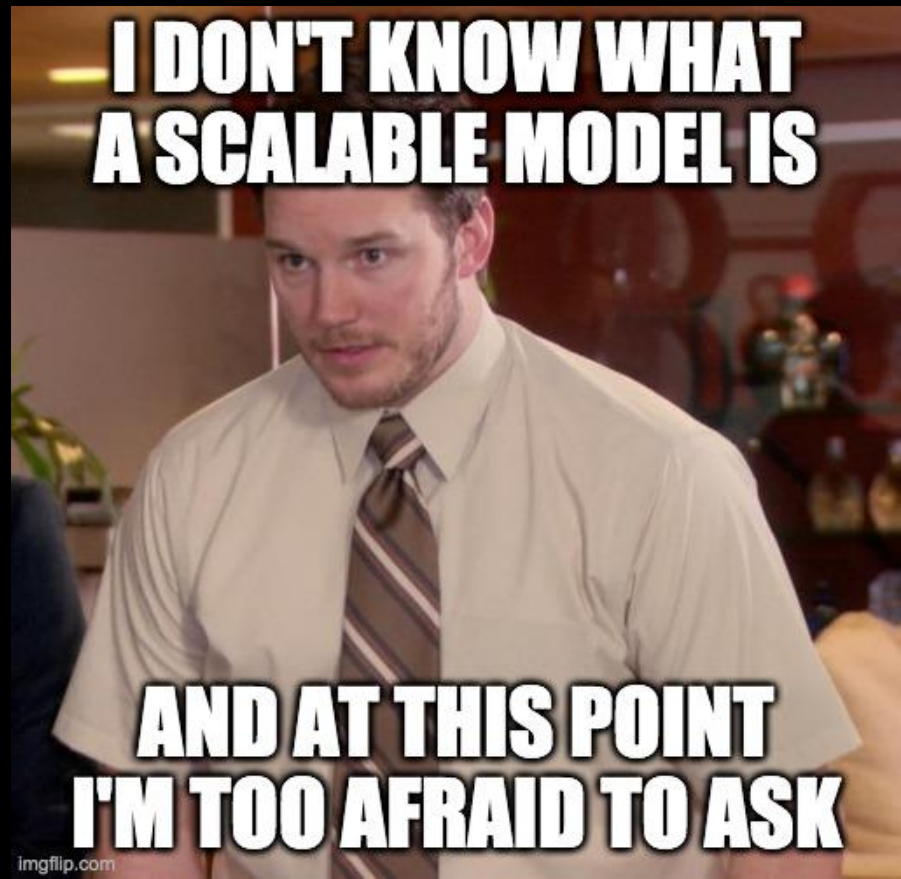
Examples:
Kubernetes
F5 XCS

Scalability

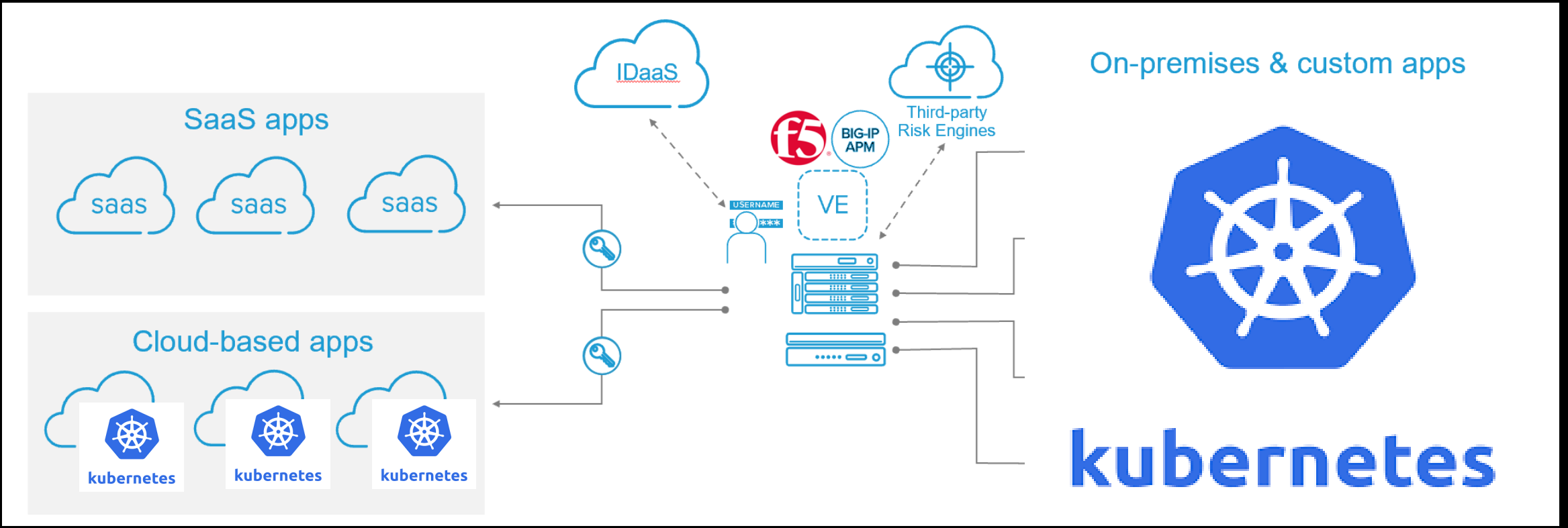
Scalability: the measure of a system's ability to increase or decrease in performance and cost in response to changes in application and system processing demands.

In IT: Can I respond, on demand, without a human involved.

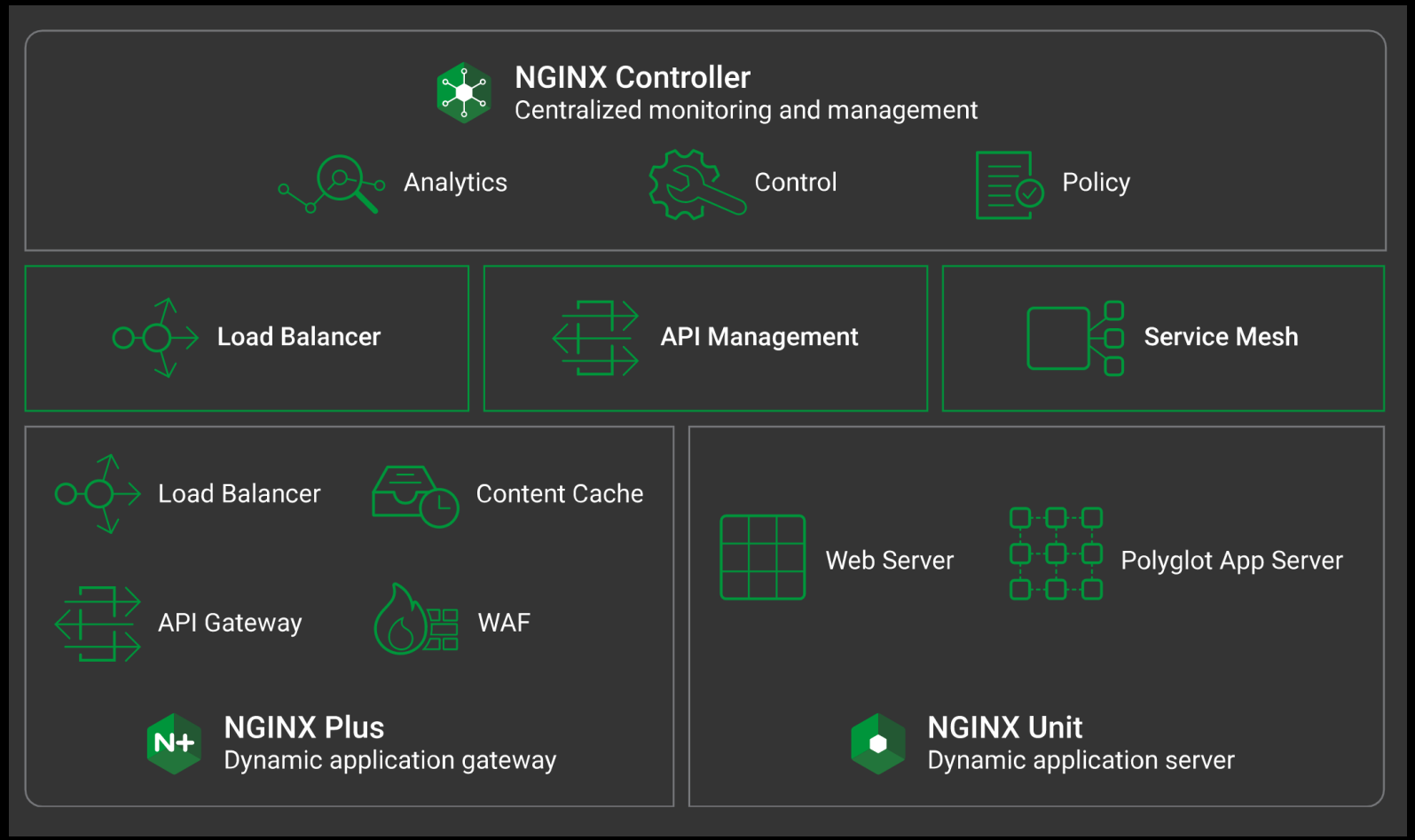
Examples:
Cloud
Kubernetes



Where Are We Headed?



Where Does NGINX+ Fit In?



- Kubernetes Ingress Controller
- Service Mesh
- API Gateway
- WAF - NGINX App Protect
- ADC / RWP
- Web Server
- Caching
- OIDC Integration

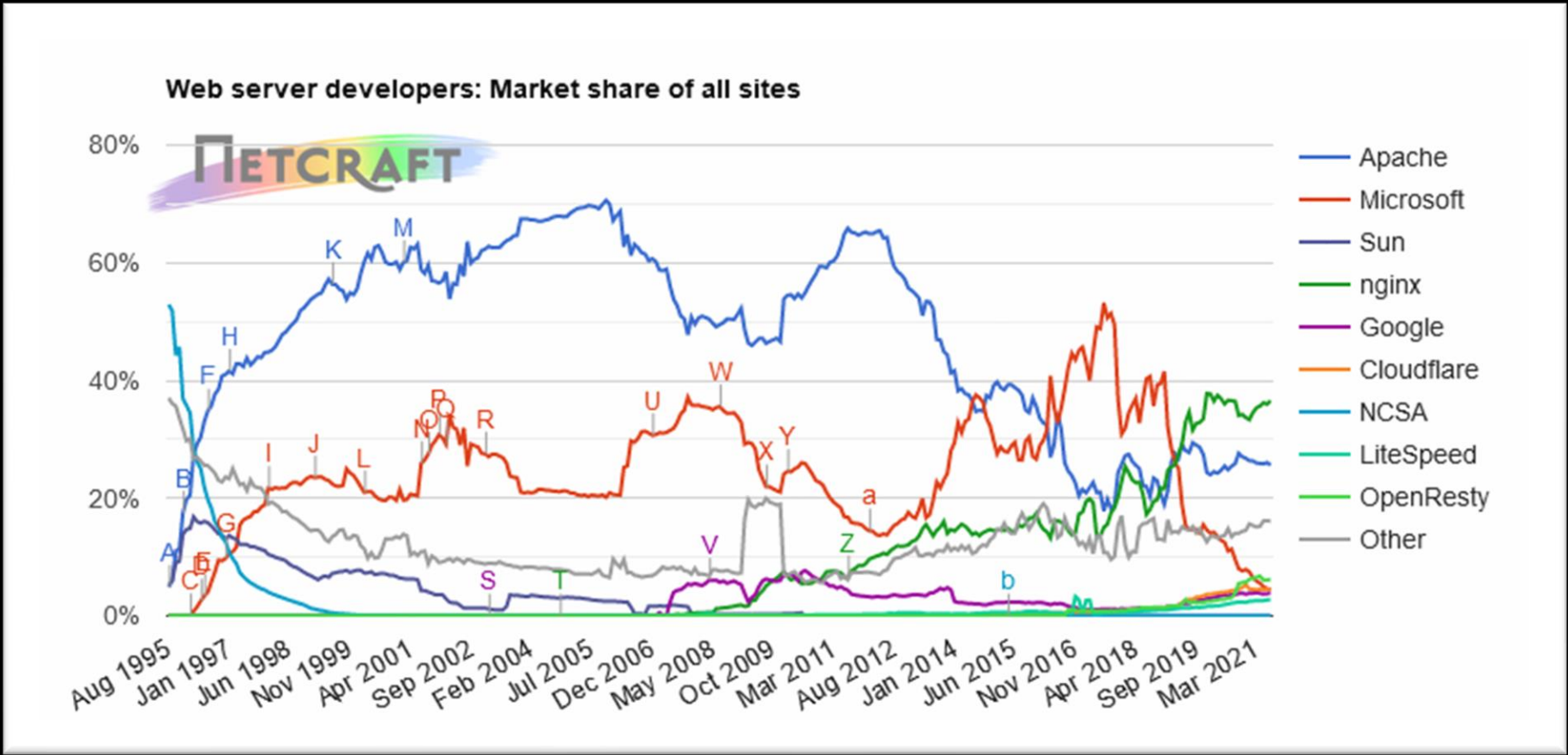
NGINX+ Web Server Dominance

Application Architects choose NGINX for:

- Security/Trust/Reputation
- Performance
- Scalability
- Form-factor

Reduce Complexity:

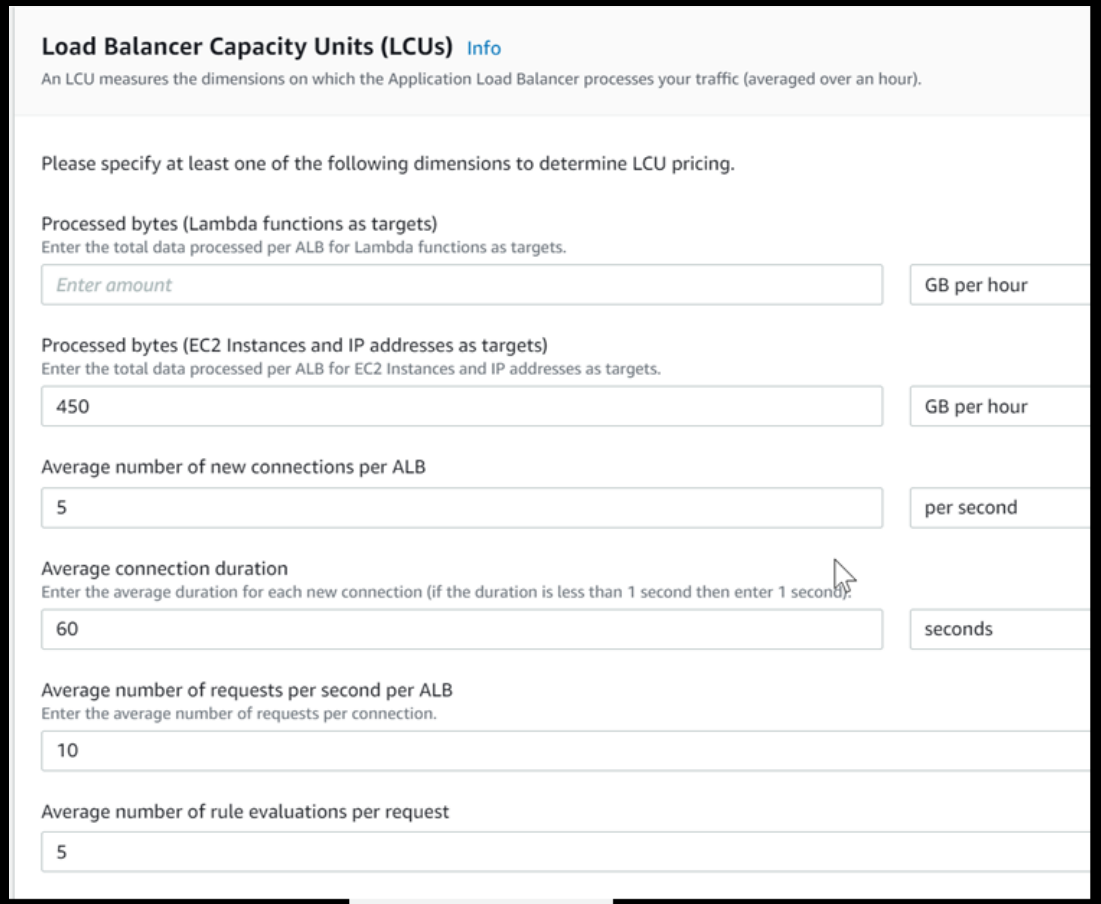
- Load Balancer
- Reverse-Proxy
- Web App Firewall
- API Gateway



Source: https://news.netcraft.com/archives/2021/07/26/july-2021-web-server-survey.html

NGINX+ SW Load Balancer

- Widely Deployed as OSS in AWS
  - ALB
  - NLB
- Widely Deployed as OSS in Azure
  - ALB
  - ILB
- No advanced Feature Support:
  - No RegEx URL Routing
  - No URI Rewrites
  - No TLS 1.3
  - 25 TLS Cert Limit
  - No Rate Limiting
  - No GeoLocation
  - No Auth
  - No API Gateway



Per month:

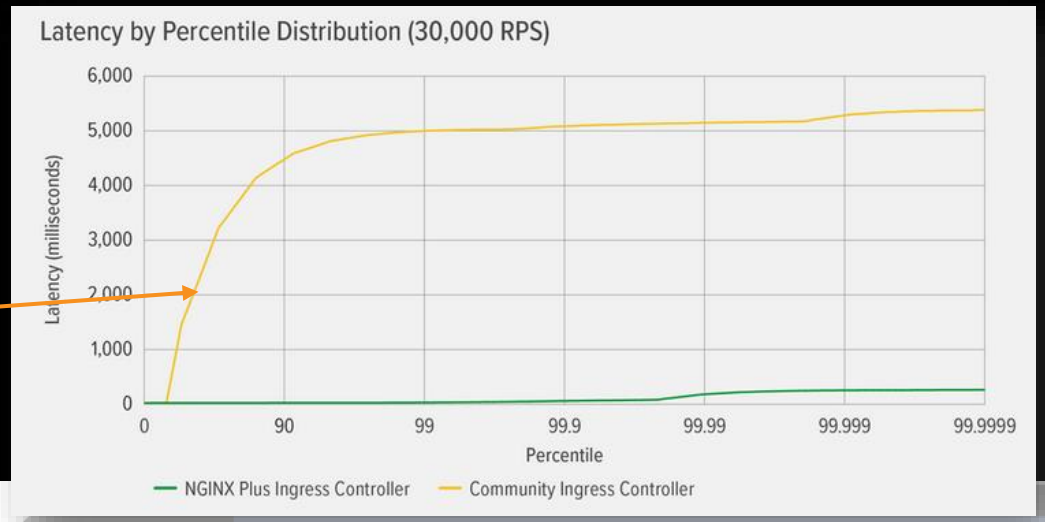
23.36 USD
3,285.00 USD
3,308.36 USD

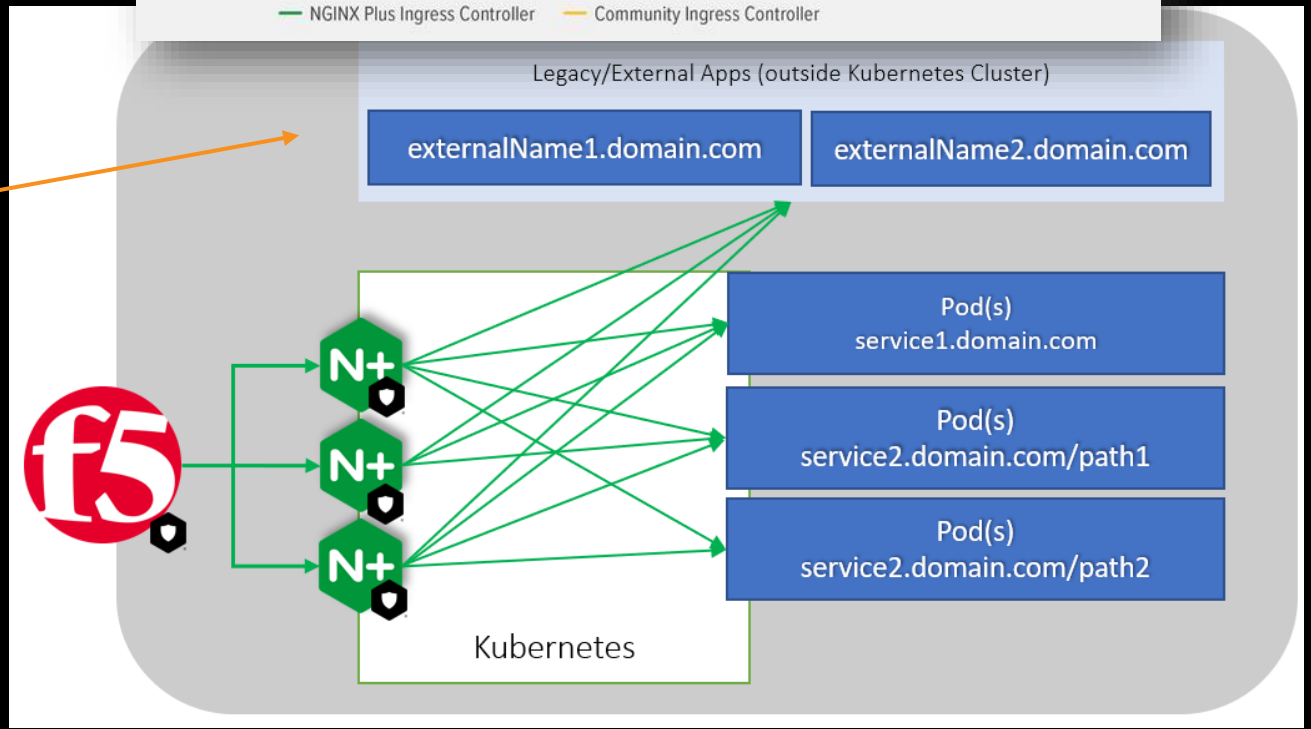
Per year: $39,696

NGINX+ Ingress Controller

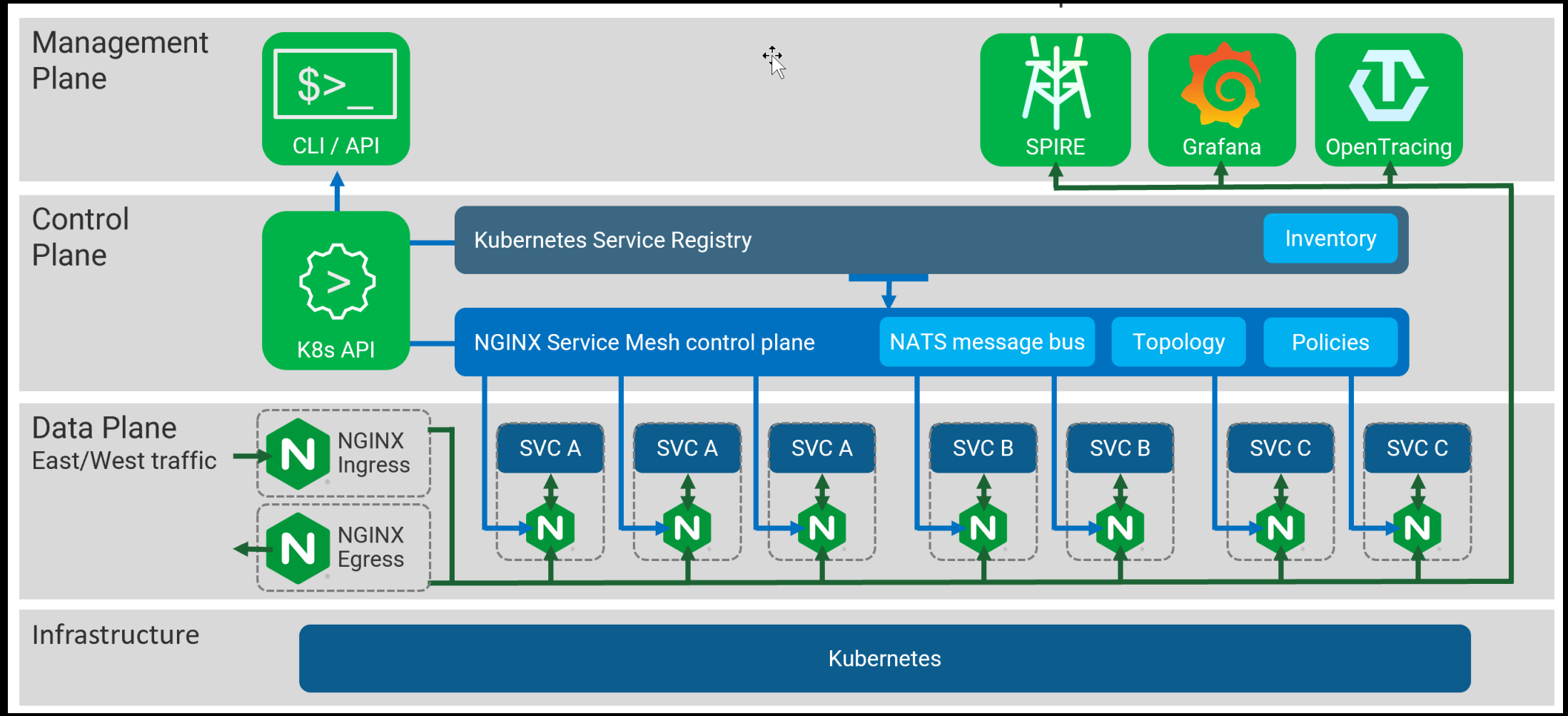
- Features and functionality exclusive to NGINX Plus

1. Real-time monitoring
2. Dynamic reconfiguration for enterprise scalability
3. Active health-checks
4. Authentication
5. Session persistence
6. Web Application Firewall
7. Support ExternalName Service





NGINX Service Mesh

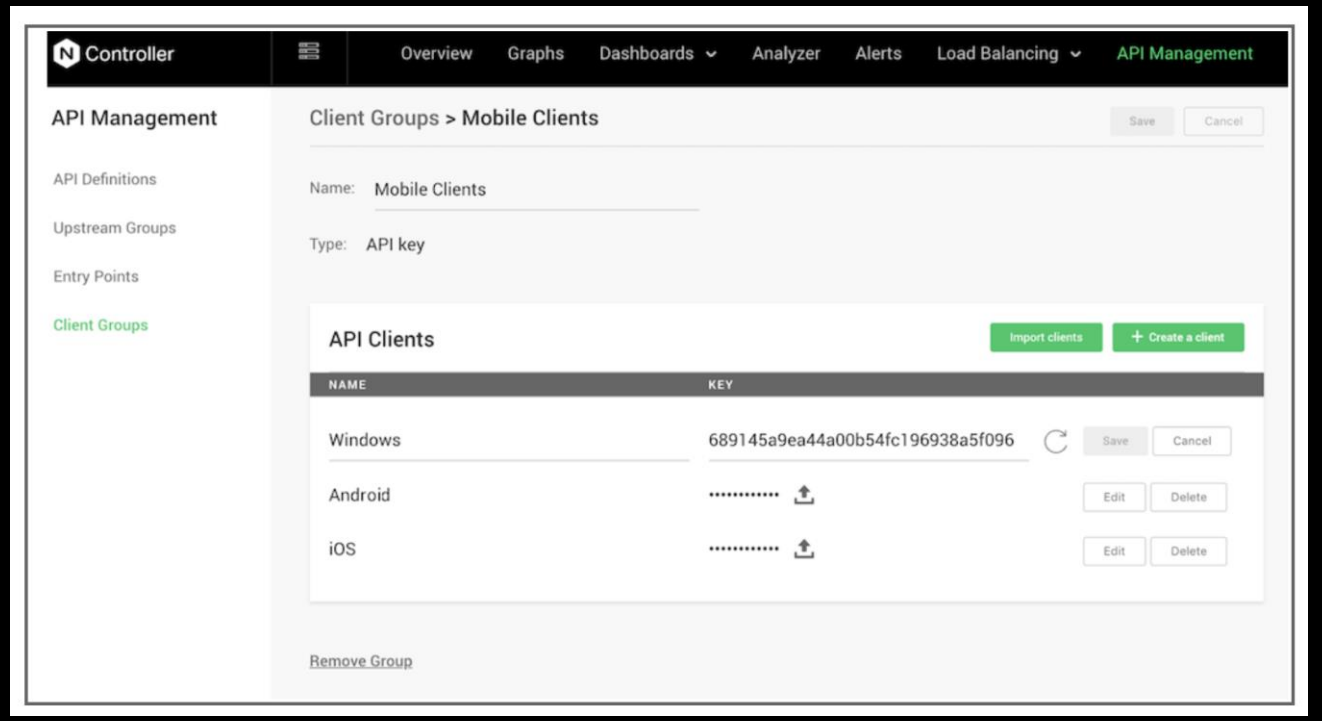


NGINX+ API Gateway

API Parameters, API Auth, Rate-limiting, Open API Spec, WAF

```
include api_backends.conf;
include api_keys.conf;

limit_req_zone $binary_remote_addr zone=client_ip_10rs:1m rate=1r/s;
limit_req_zone $http_apikey        zone=apikey_200rs:1m   rate=200r/s;

server {
    access_log /var/log/nginx/api_access.log main;  # Each API may also
                                                    # log to a separate file

    listen 443 ssl;
    server_name api.example.com;

    # TLS config
    ssl_certificate        /etc/ssl/certs/api.example.com.crt;
    ssl_certificate_key    /etc/ssl/private/api.example.com.key;
    ssl_session_cache      shared:SSL:10m;
    ssl_session_timeout    5m;
    ssl_ciphers            HIGH:!aNULL:!MD5;
    ssl_protocols          TLSv1.2 TLSv1.3;

    # API definitions, one per file
    include api_conf.d/*.conf;

    # Error responses
    error_page 404 = @400;         # Treat invalid paths as bad requests
    proxy_intercept_errors on;     # Do not send backend errors to client
    include api_json_errors.conf;  # API client-friendly JSON errors
    default_type application/json; # If no content-type, assume JSON
}
```

API Authentication Methods:
API Key
OIDC Connect w/JWT
SAML



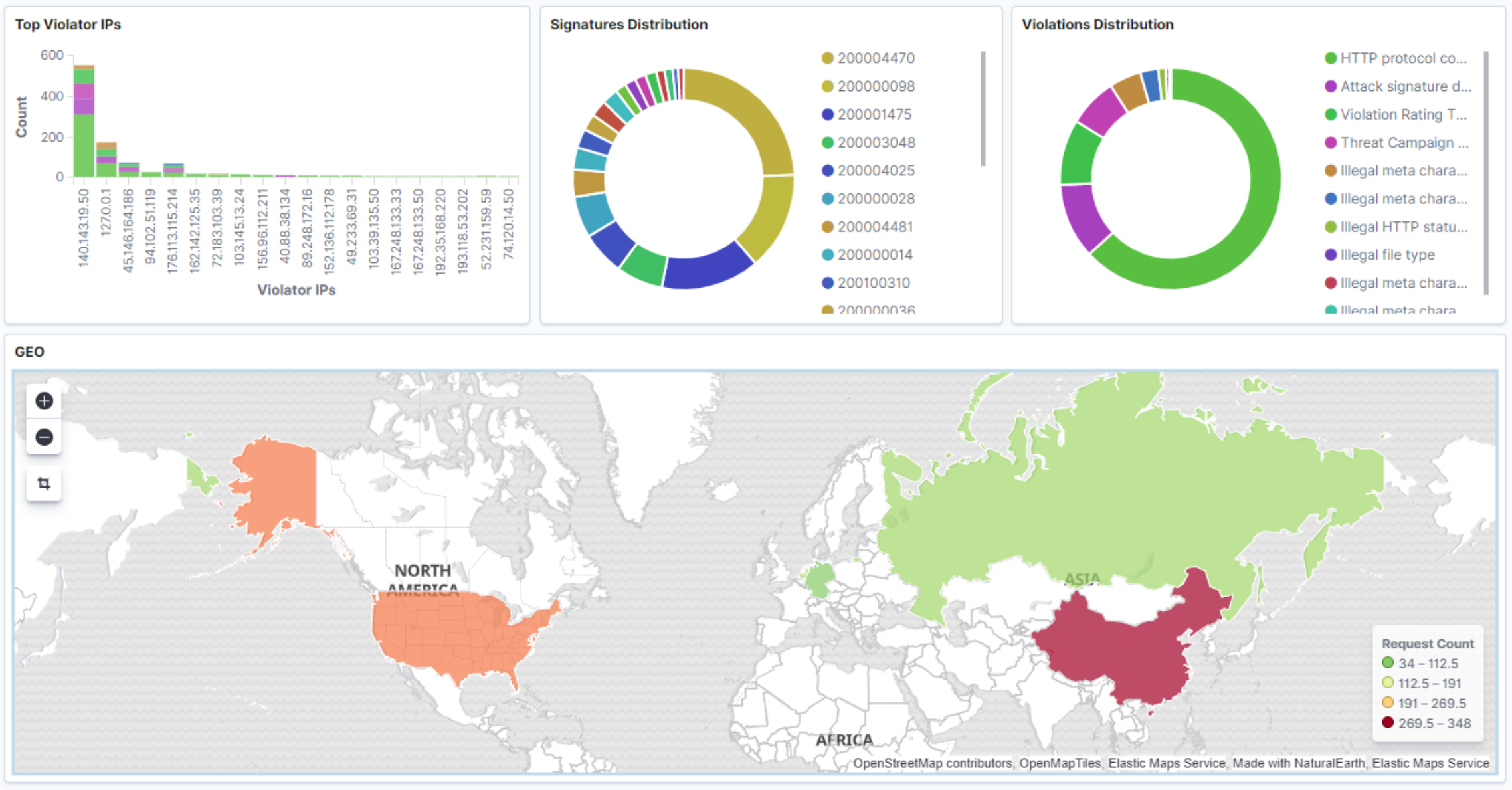
NGINX+ API Gateway & WAF

NAP is CI/CD Friendly

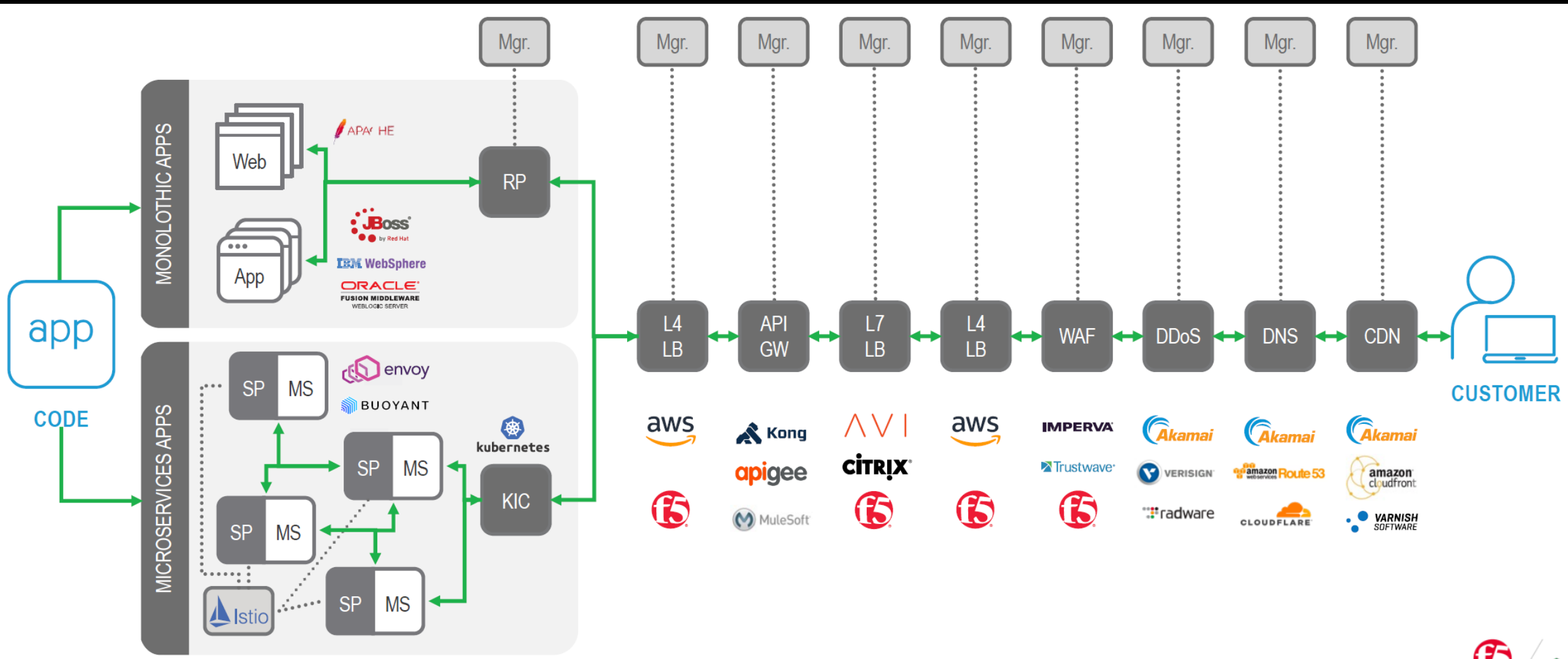
```
http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;

    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;
        }
    }
```

```
{
    "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"
        }
    ]
}
```

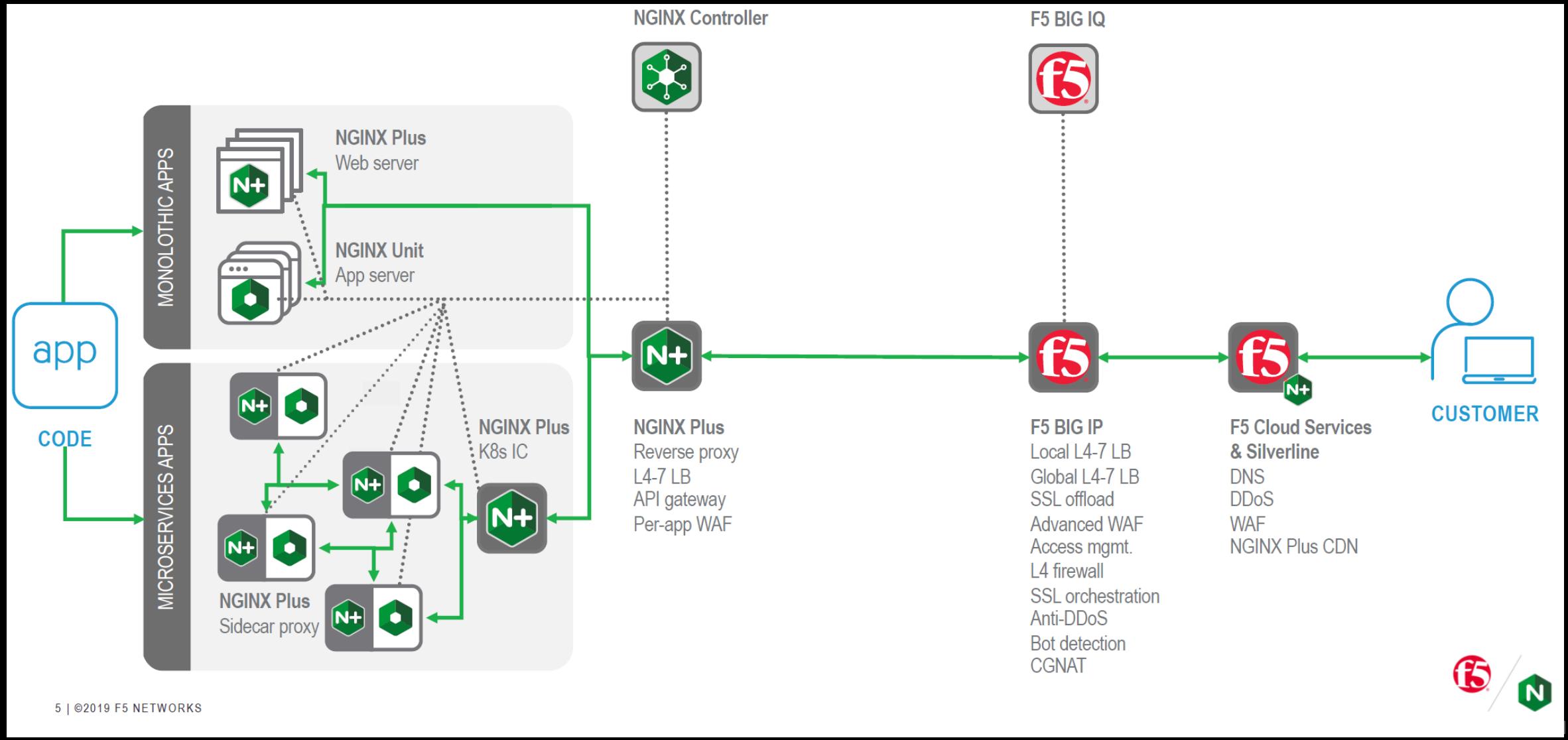
NGINX+ API & WAF Visibility



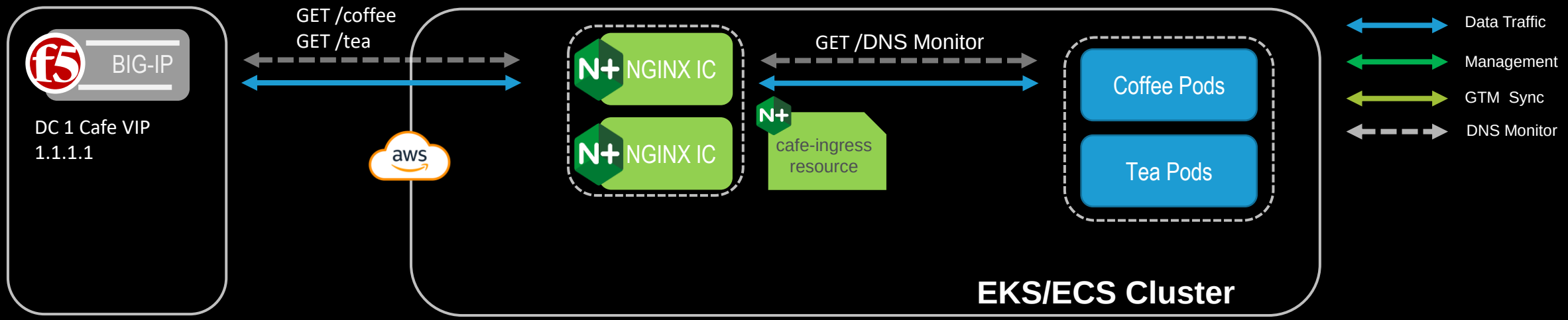
NGINX+ – Today, a Patchwork of Tools



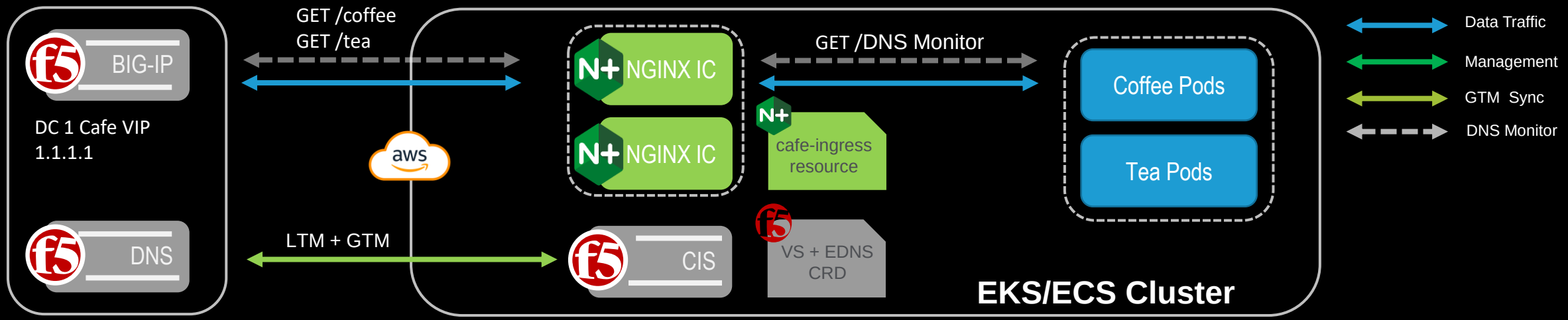
NGINX+ & BIG-IP! 13 Tools Down to 3



Multi-Cluster Multi-Site with IngressLink

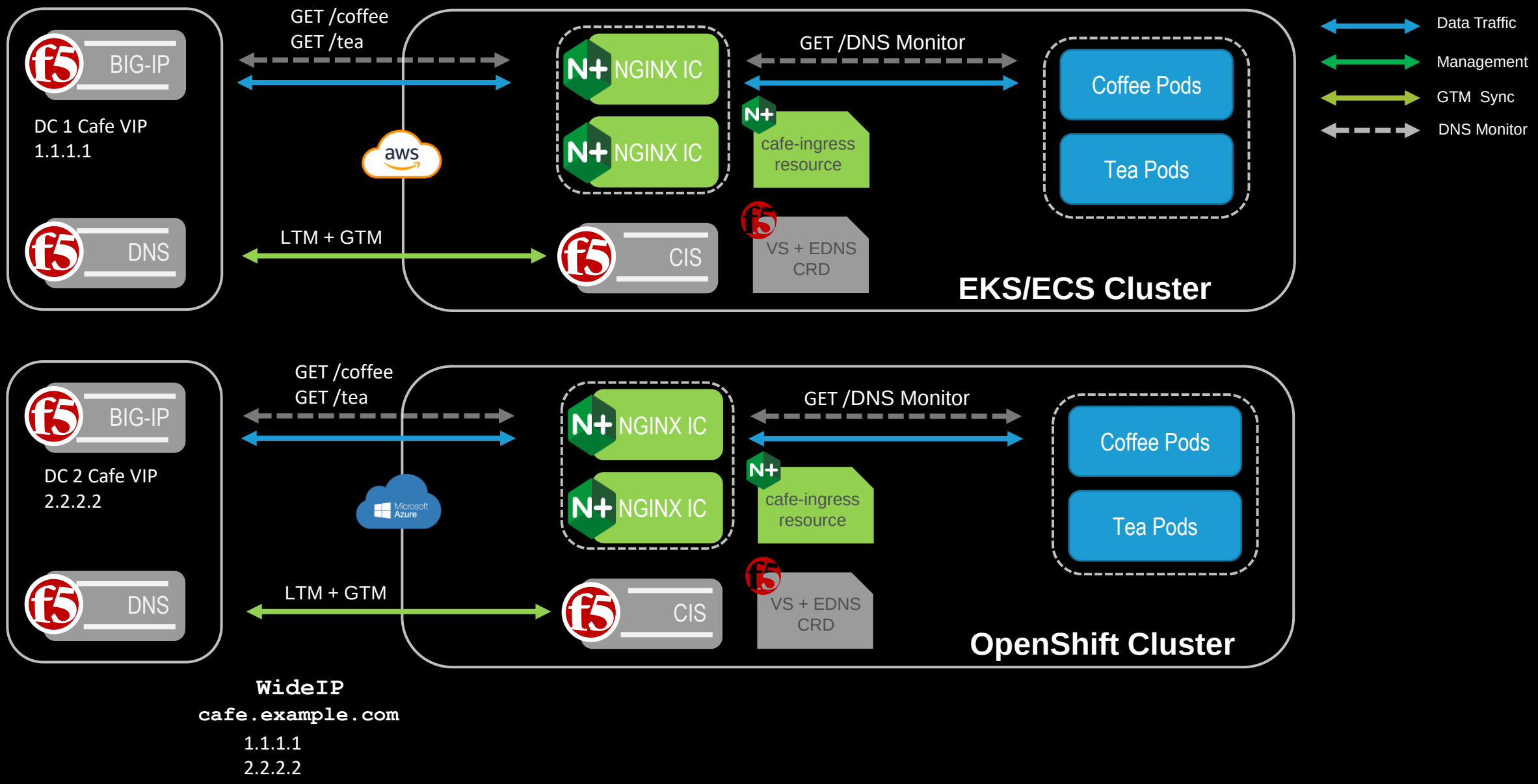


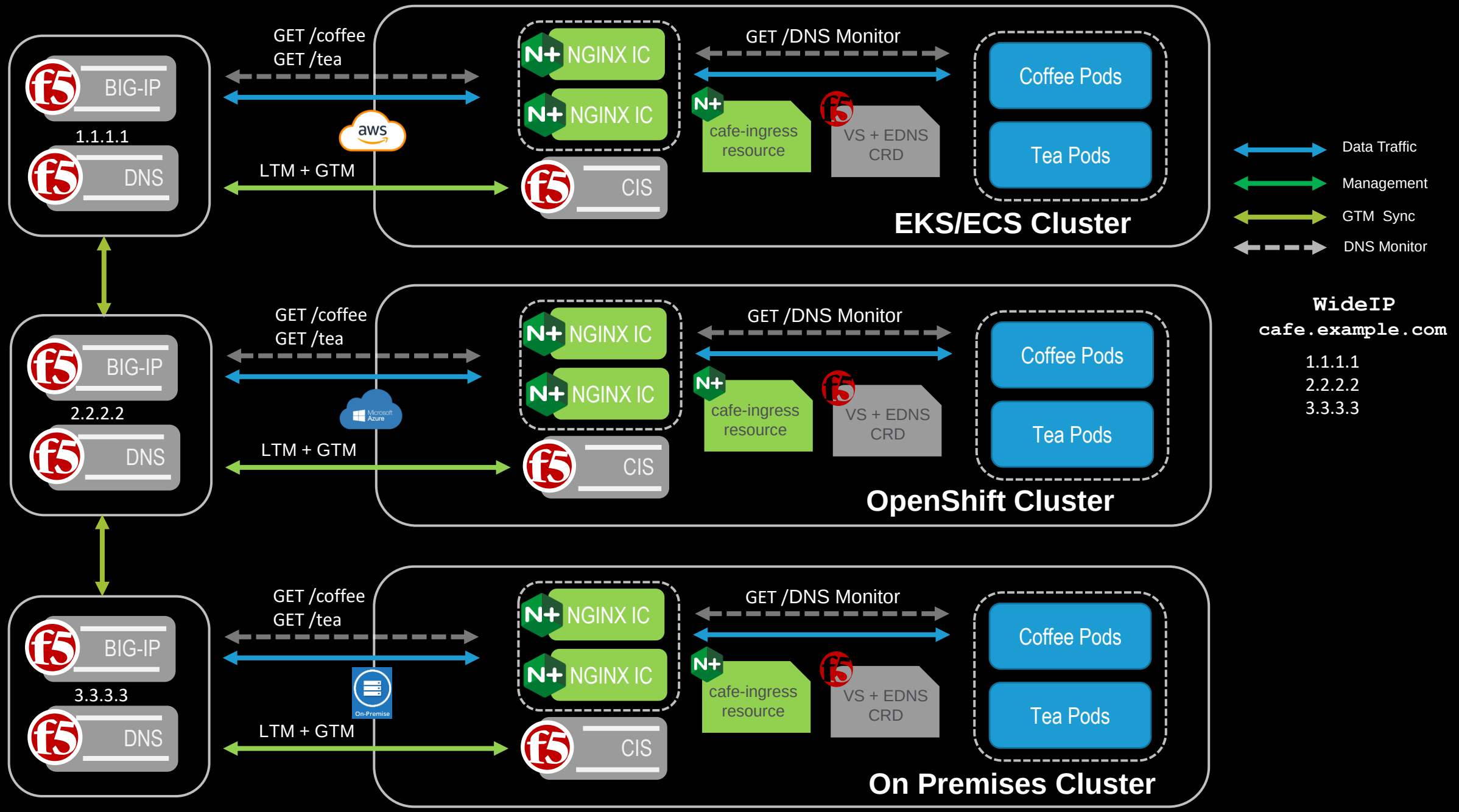
Multi-Cluster Multi-Site with IngressLink



WideIP
cafe.example.com
1.1.1.1

Multi-Cluster Multi-Site with IngressLink

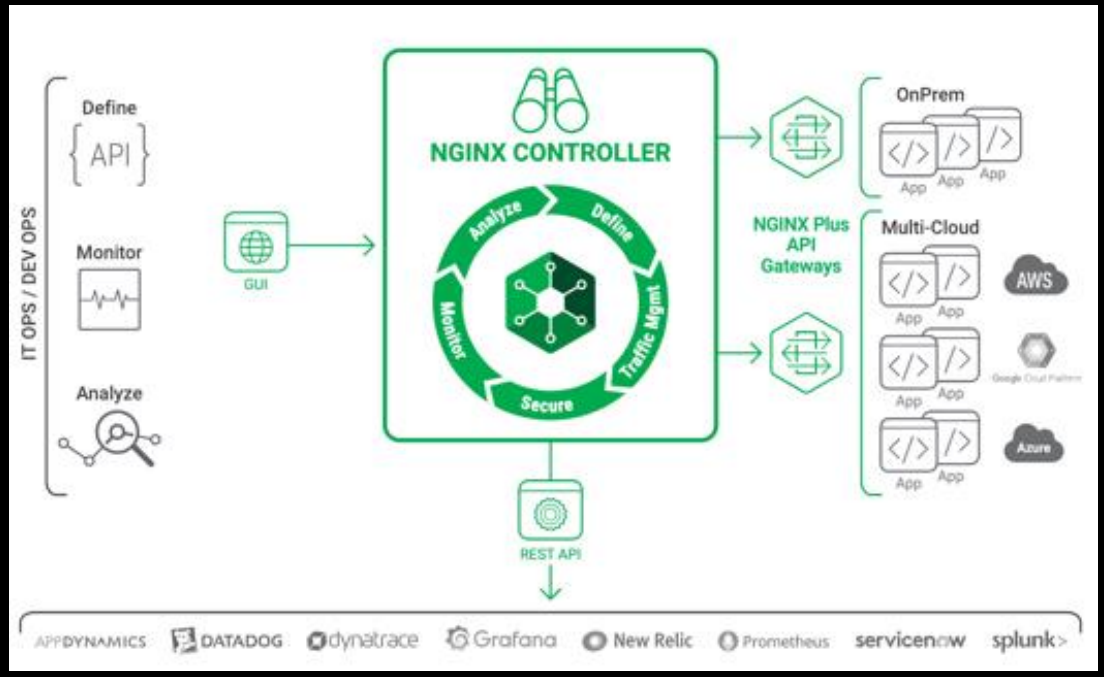


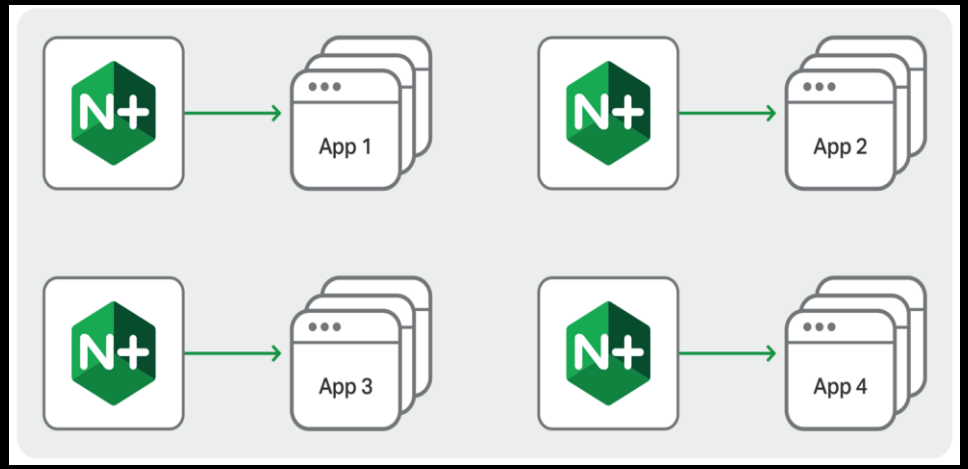

BIG-IP
1.1.1.1
DNS
GET /coffee
GET /tea
aws
LTM + GTM
NGINX IC
NGINX IC
CIS
GET /DNS Monitor
cafe-ingress resource
VS + EDNS CRD
Coffee Pods
Tea Pods
EKS/ECS Cluster
Data Traffic
Management
GTM Sync
DNS Monitor
BIG-IP
2.2.2.2
DNS
GET /coffee
GET /tea
Microsoft Azure
LTM + GTM
NGINX IC
NGINX IC
CIS
GET /DNS Monitor
cafe-ingress resource
VS + EDNS CRD
Coffee Pods
Tea Pods
OpenShift Cluster
WideIP
cafe.example.com
1.1.1.1
2.2.2.2
3.3.3.3
BIG-IP
3.3.3.3
DNS
GET /coffee
GET /tea
On-Premise
LTM + GTM
NGINX IC
NGINX IC
CIS
GET /DNS Monitor
cafe-ingress resource
VS + EDNS CRD
Coffee Pods
Tea Pods
On Premises Cluster

What is NGINX Plus?

ENTERPRISE SOLUTIONS WITH DYNAMIC MODULES

- Enterprise class visibility with 90+ additional metrics
- JWT Authentication
- Native OpenID Connect support
- Active health checks on status code and response body
- Service discovery using DNS
- Key value store (dynamic IP black-listing, blue/green deployments)
- Dynamic reconfiguration—zero downtime
- Session persistence based on cookie
- HA Configuration
- Dashboard built in





https://www.nginx.com/products/nginx/#compare-versions

Questions?