



F5 Synthesis Information Session

April, 2014



Agenda

- Welcome and Introduction to Customer Technology Challenges
- Software Defined Application Services
- Reference Architectures for Today's Customer Challenges
- Total Cost of Ownership and New Business Models
- Multi-network Environment and Partner Ecosystem
- Making it Happen with Global Services
- Q & A

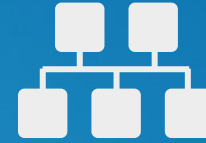
Technology Shifts Are Creating Opportunity



SDDC/Cloud



Advanced threats



“Software defined”
everything



Internet of
Things



Mobility



HTTP is the
new TCP

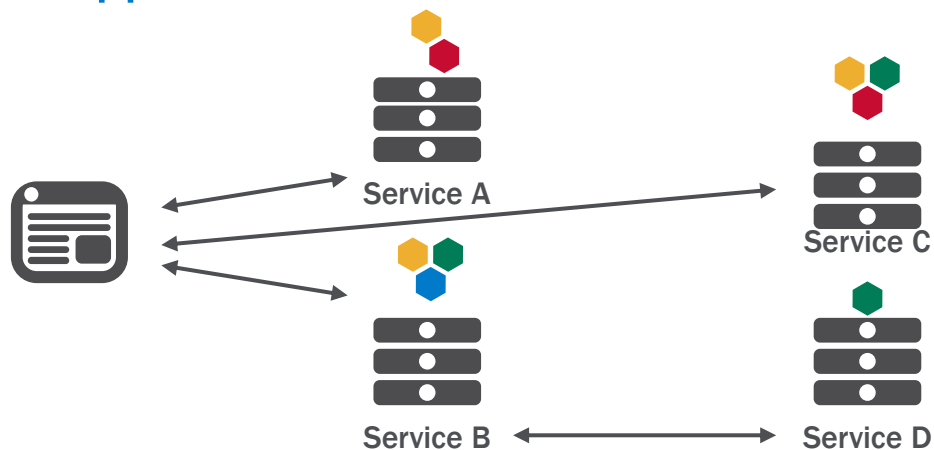
Impact on Data Center Architecture: Applications

MICRO-ARCHITECTURES

Each service is isolated and requires its own:

- Load balancing
- Authentication / authorization
- Security
- Layer 7 Services
- May be API-based, expanding services required

More applications need services

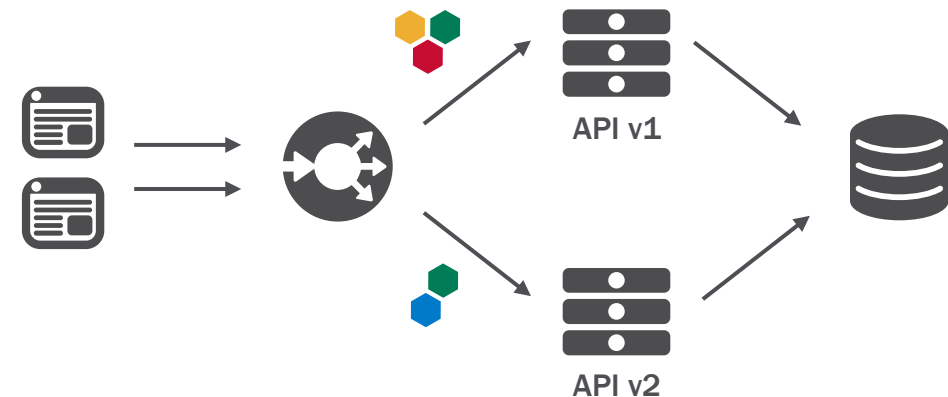


API DOMINANCE

Proxies are used in emerging API-centric architectures for:

- API versioning
- Client-based steering
- API Load balancing
- Metering & billing
- API key management

More intelligence needed in services

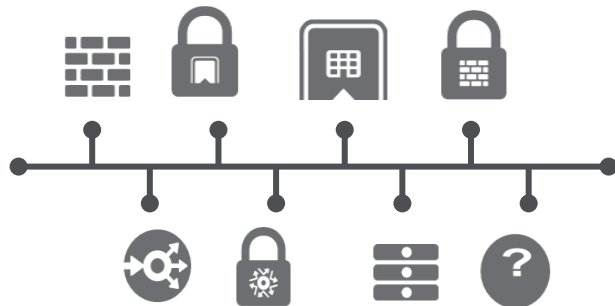


Impact on Data Center Architecture: Network

SOLUTION SPRAWL

Increasing threats and client platforms result in need for:

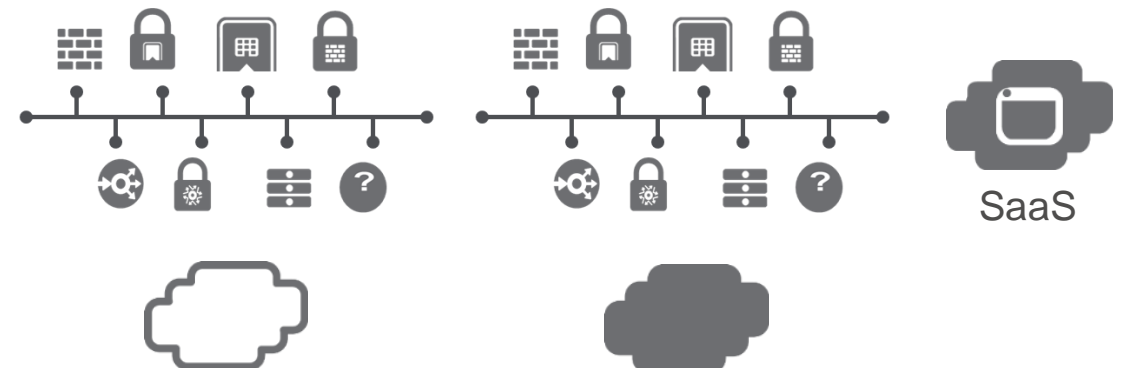
- Mobile device management
- Mobile access management
- Mobile security
- DDoS
- Application layer threats
- Malware



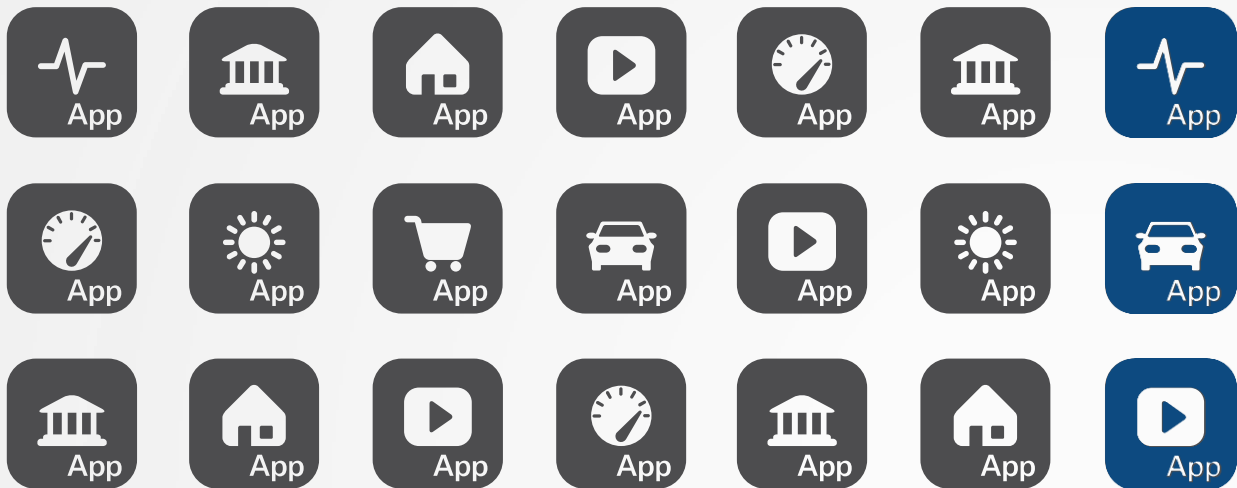
OPERATIONAL INCONSISTENCY

Introduction of off-premise cloud solutions without architectural parity results in:

- Inconsistent enforcement of business and operational policies
- Unpredictable application performance and security
- Increased OpEx as new management paradigms are introduced



“Leave No Application Behind”



1000
Average number of applications deployed within an enterprise

DDoS

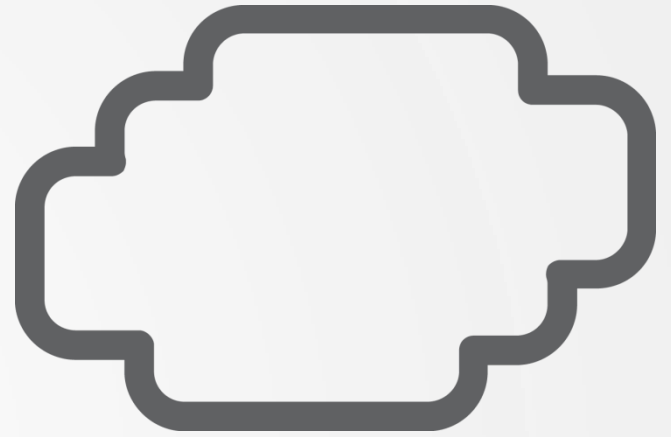
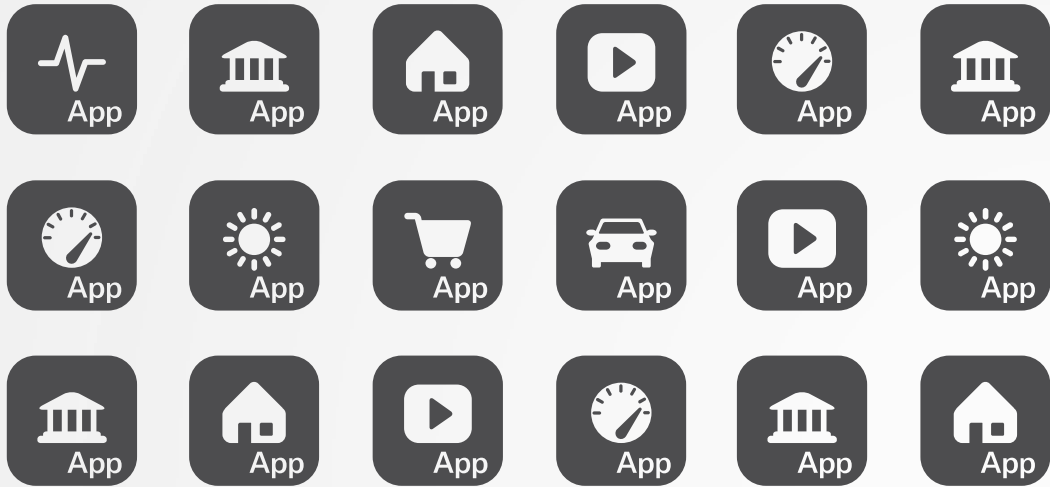
WAF

SSL

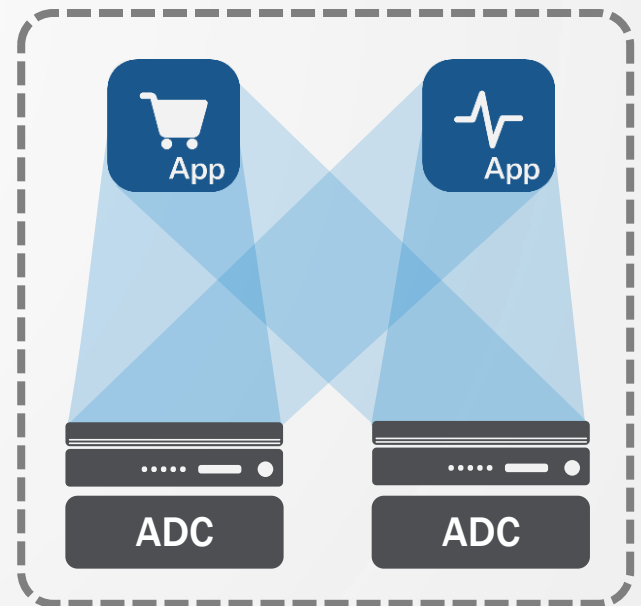
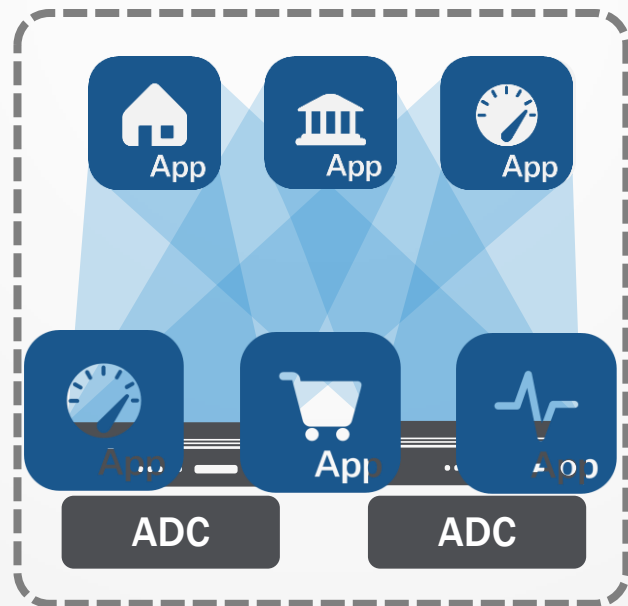
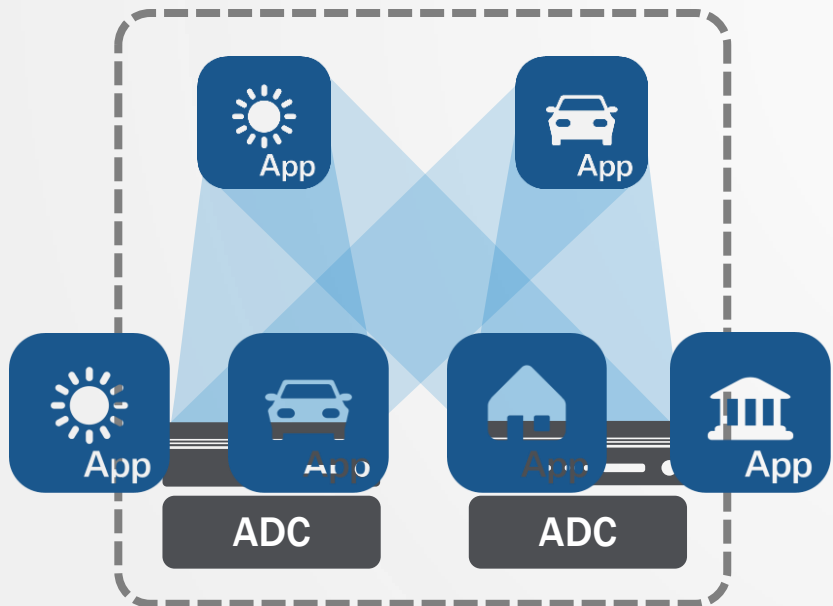
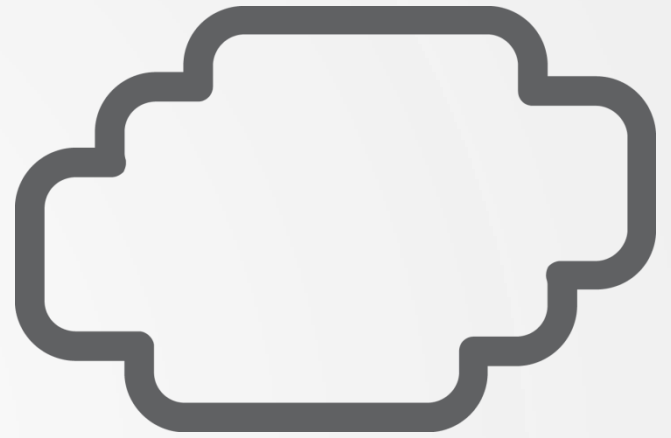
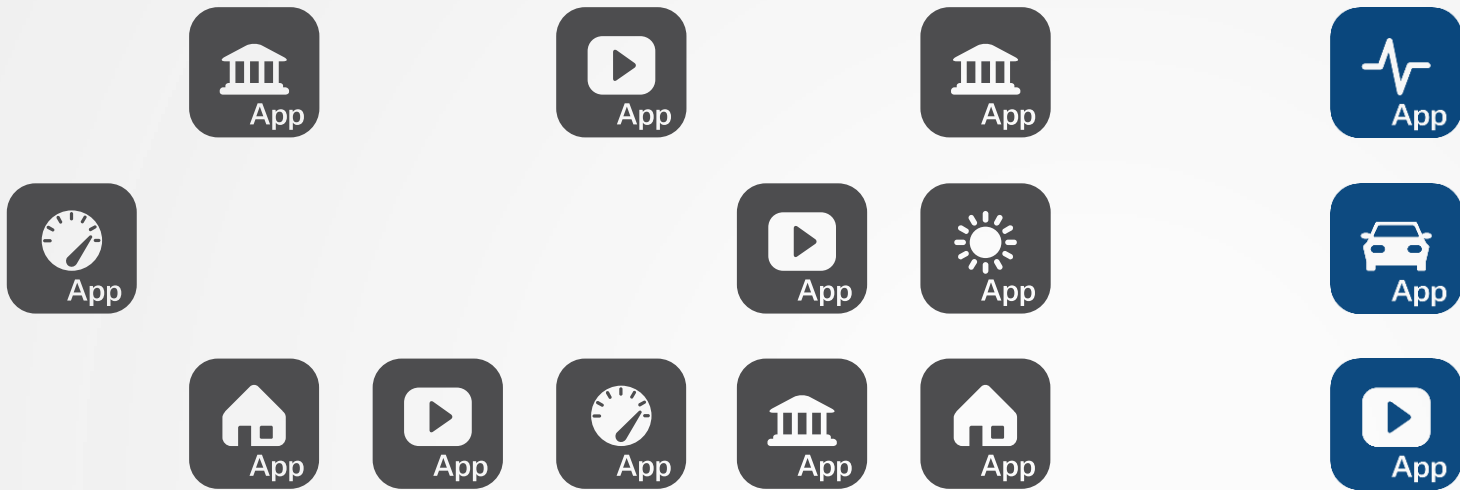
Acceleration

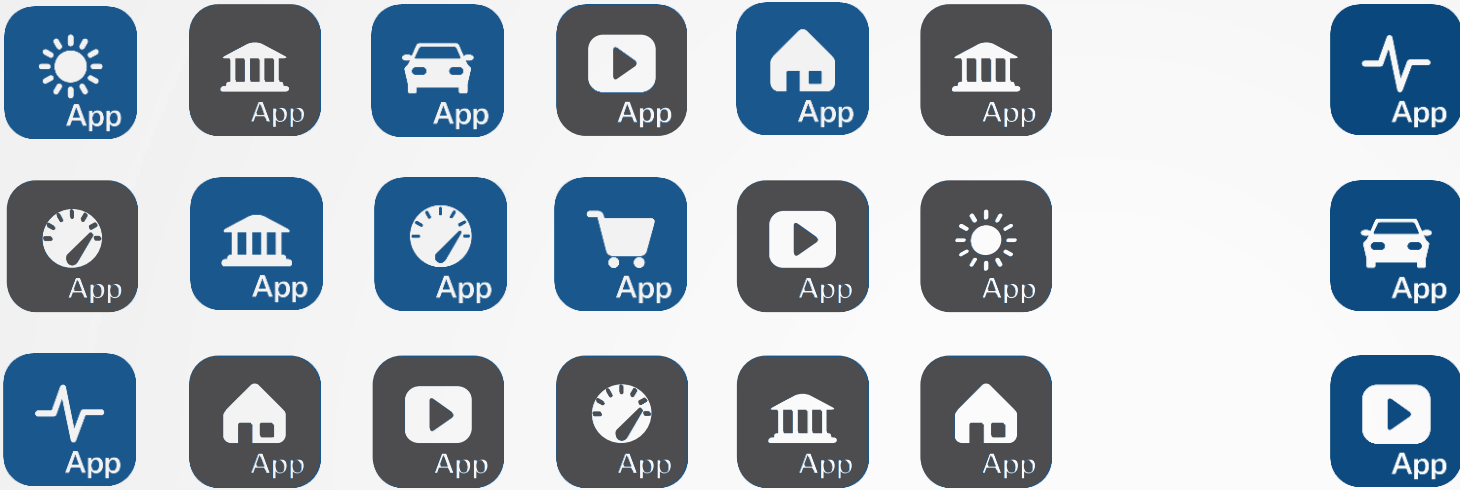
LTE

Applications require services



The selected few





The graphic consists of four overlapping, semi-transparent, rounded shapes in blue, yellow, red, and green. Each shape has a fine grid pattern overlaid on it. The shapes overlap in the center, creating a bright white glow.

f5 Synthesis™

The 4th Phase of the Evolution

f5 Synthesis™

4

Software Defined Application Services

3

Cloud Ready

2

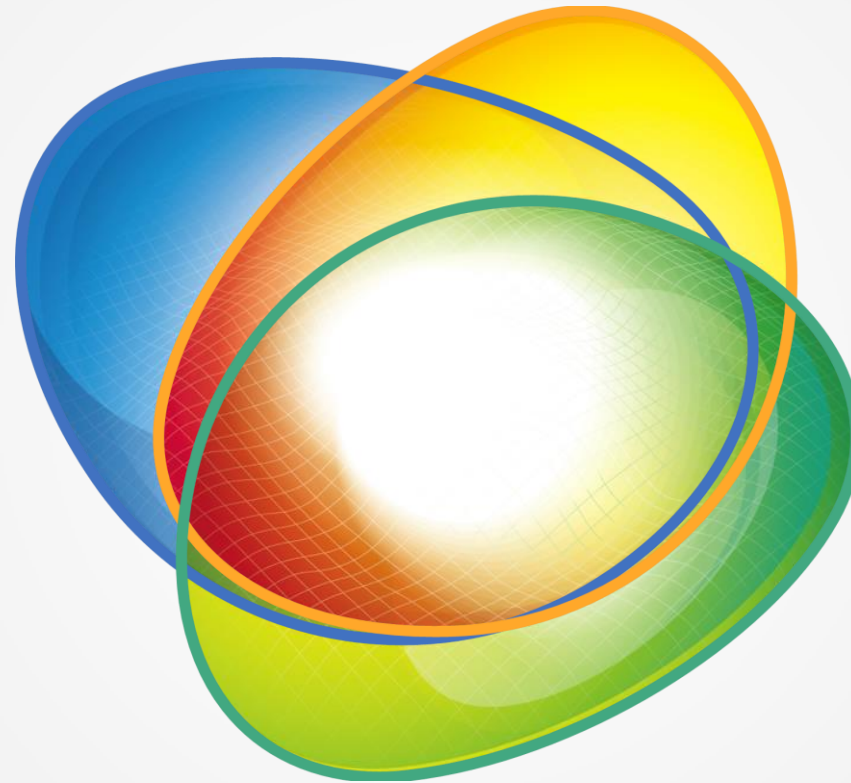
Broadened Application Services

1

Application Delivery Controller

Software Defined Application Services Elements

High-Performance
Services Fabric

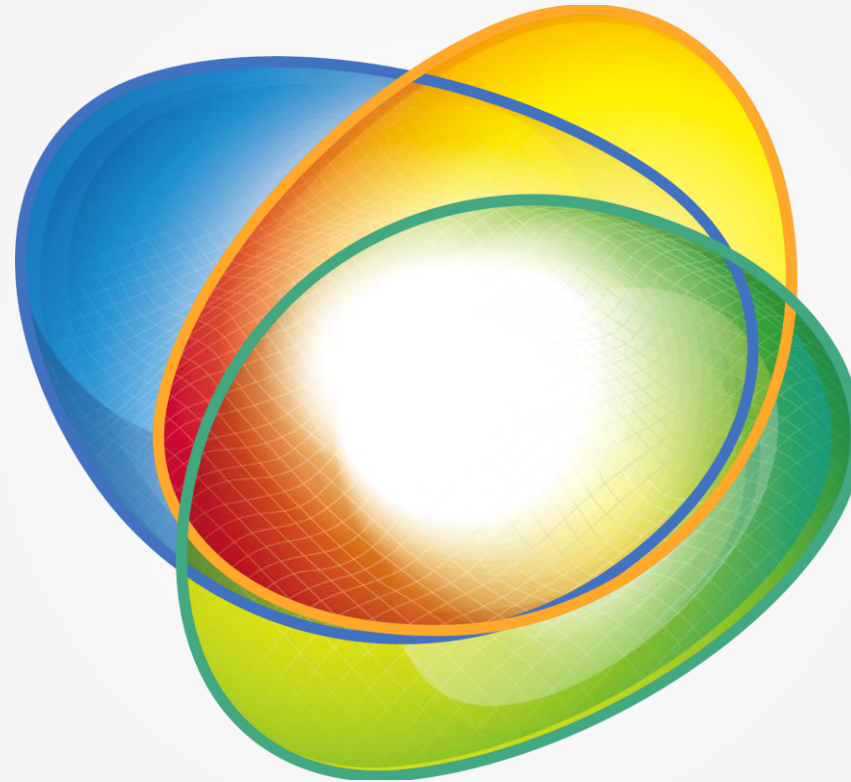


Intelligent
Services Orchestration

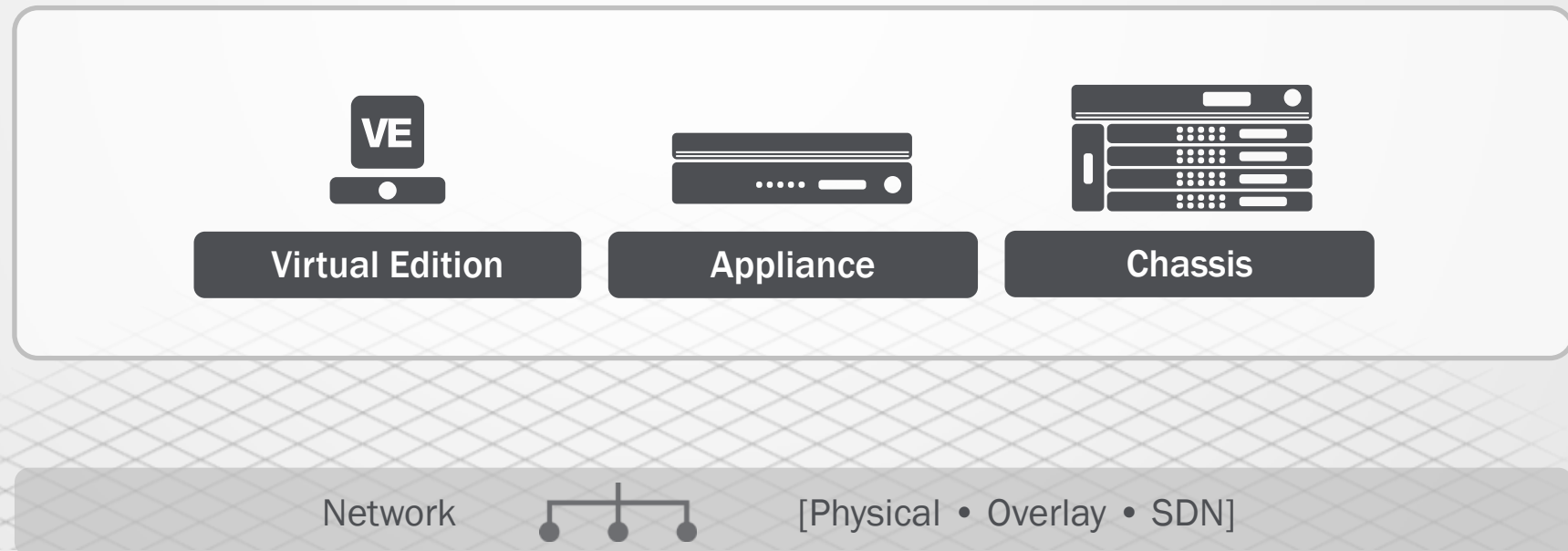
Simplified
Business Models

Software Defined Application Services Elements

High-Performance
Services Fabric



High-Performance Services Fabric

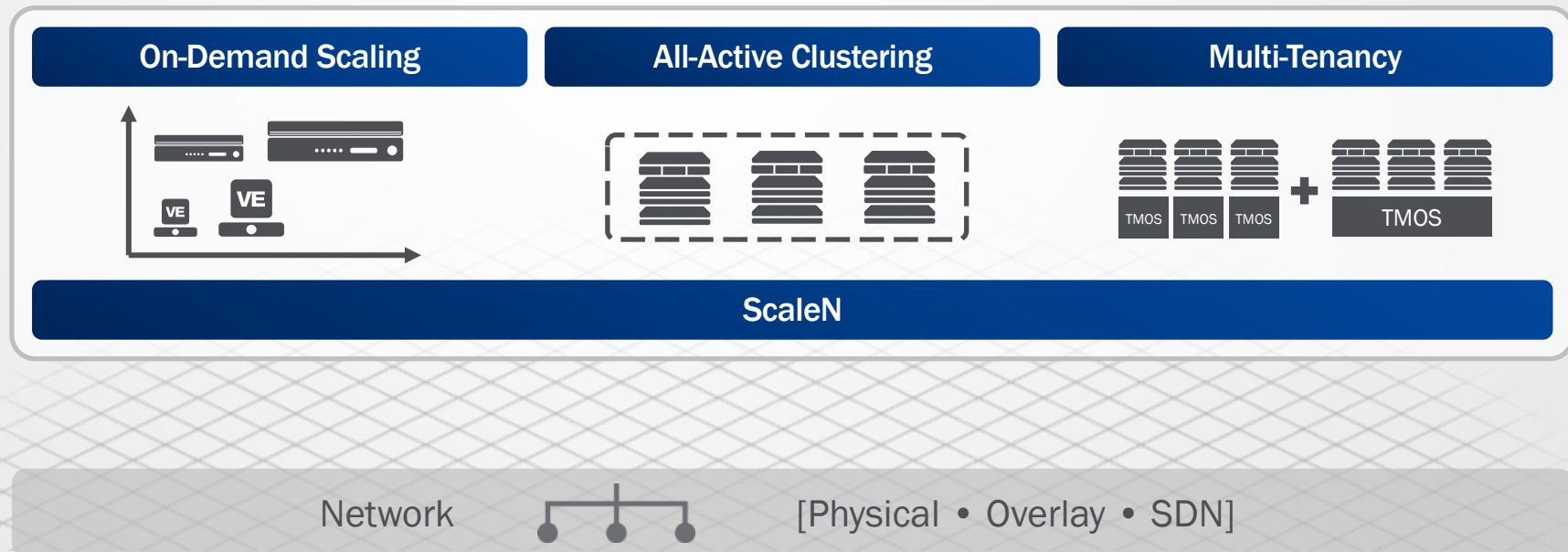


High-Performance Services Fabric

Elastic, multi-tenant
platform

All-active

Application-aware



High-Performance Services Fabric

Elastic, multi-tenant platform

All-active

Application-aware

Performance leader

20Tbps

Throughput

320M

Connections per second

9.2B

Concurrent connections

80*

Multi-tenant instances per device

32

Device service clusters

*40K when combining admin instances with vCMP

Network



[Physical • Overlay • SDN]

High-Performance Services Fabric

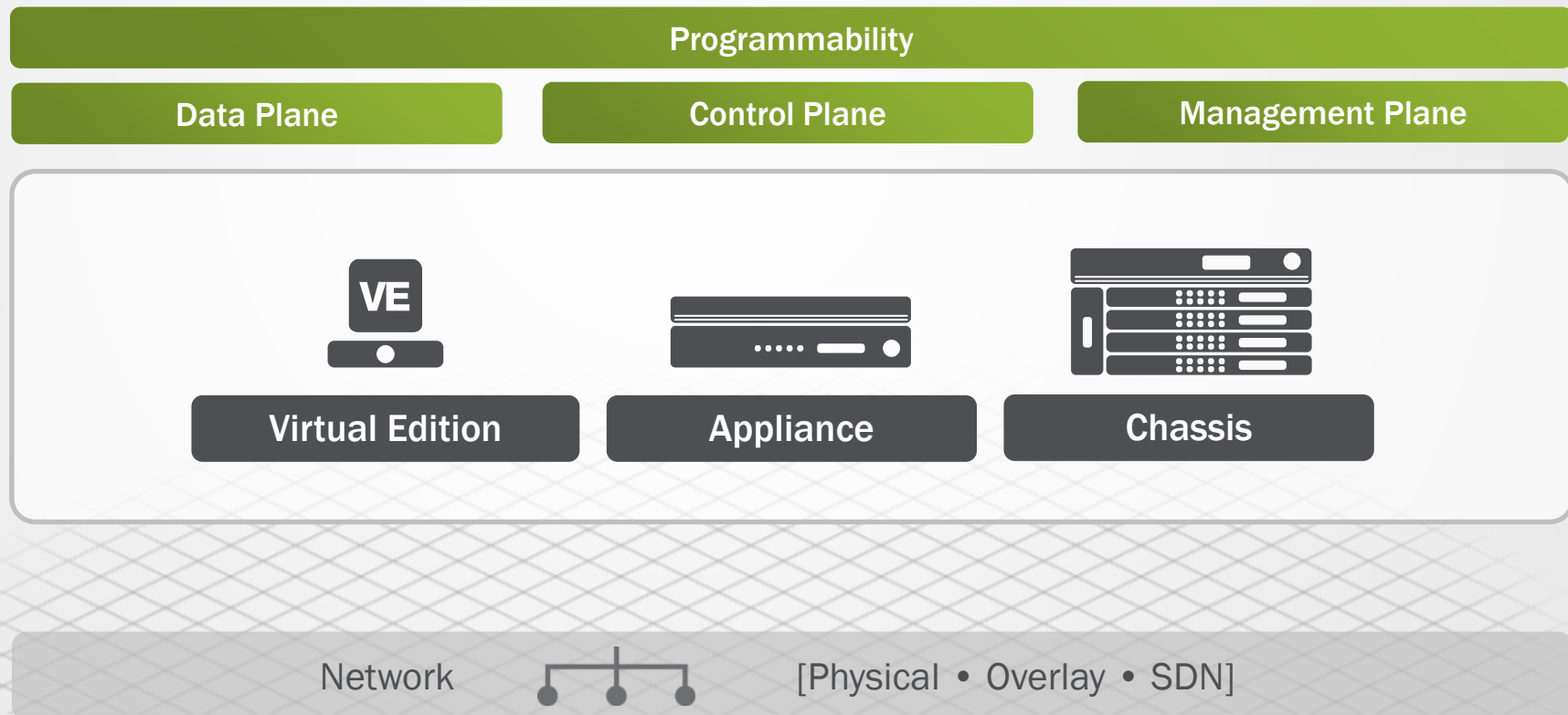
Elastic, multi-tenant platform

All-active

Application-aware

Performance leader

Extensible and programmable



High-Performance Services Fabric

Elastic, multi-tenant platform

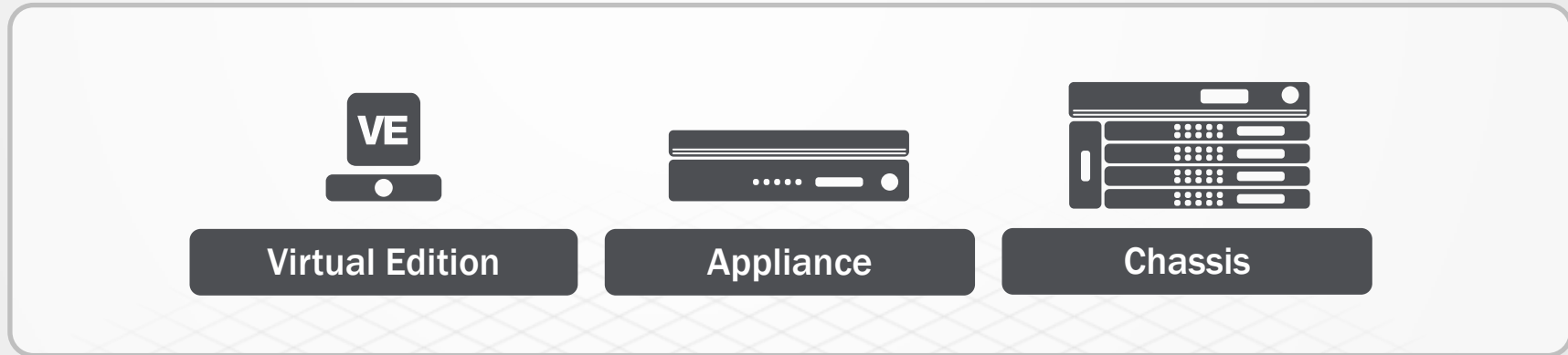
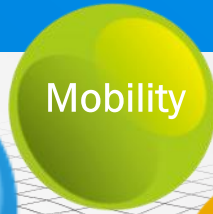
All-active

Application-aware

Performance leader

Extensible and programmable

Catalog of application services



Software Defined Application Services

Software Defined Application Services

Service Provider
and Enterprise

Device, Network
and Applications

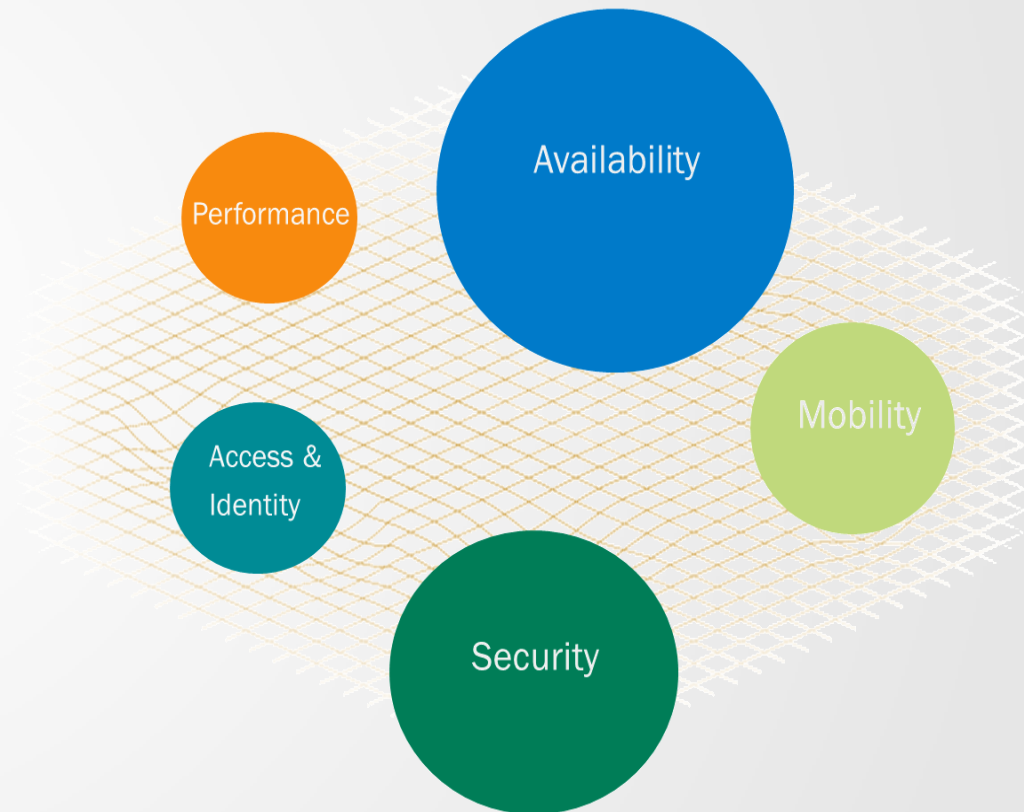
Performance
and Scale

Extensible and
programmable

Automation and
Orchestration

F5 Software Defined Application Services (SDAS)

A rich set of services that address
the delivery challenges faced by
businesses today.



Software Defined Application Services

Eliminate single points of failure

Application fault isolation

Context-aware

Elastic scale

Extensible and programmable

Public, private and hybrid cloud

Global Server LB **Load Balancing**
Global Server LB **CGNAT**
Global Load Balancing **Authoritative DNS**
Disaster Recovery
Cloud Bursting **Business Continuity**
Intelligent EPC node selection
DNS Caching & Resolving



Software Defined Application Services

Any device, any user, anywhere

Performance-related protocol support

Context-aware

Cloud or data center

Compression
Traffic Management
Caching **Acceleration**
Optimization
Web Performance Optimization
SPDY Gateway
Traffic Shaping and QoS
Application Optimization



Software Defined Application Services

Single Sign-on

Identity federation

Context-aware

Endpoint inspection
and protection
against fraud

Extensible and
Programmable

Any device,
anywhere

SAML Federation
Cloud Federation
Access Control
Anti-Malware
Single Sign-On
SSL VPN
Endpoint Inspection
Active Sync Proxy
Secure Web Gateway
Web Access Management

Performance

Availability

Access &
Identity

Mobility

Security

Software Defined Application Services

Secures device,
network and
application

Protects critical
infrastructure from
disruptive attacks

Application-aware

Extends protection
into the cloud

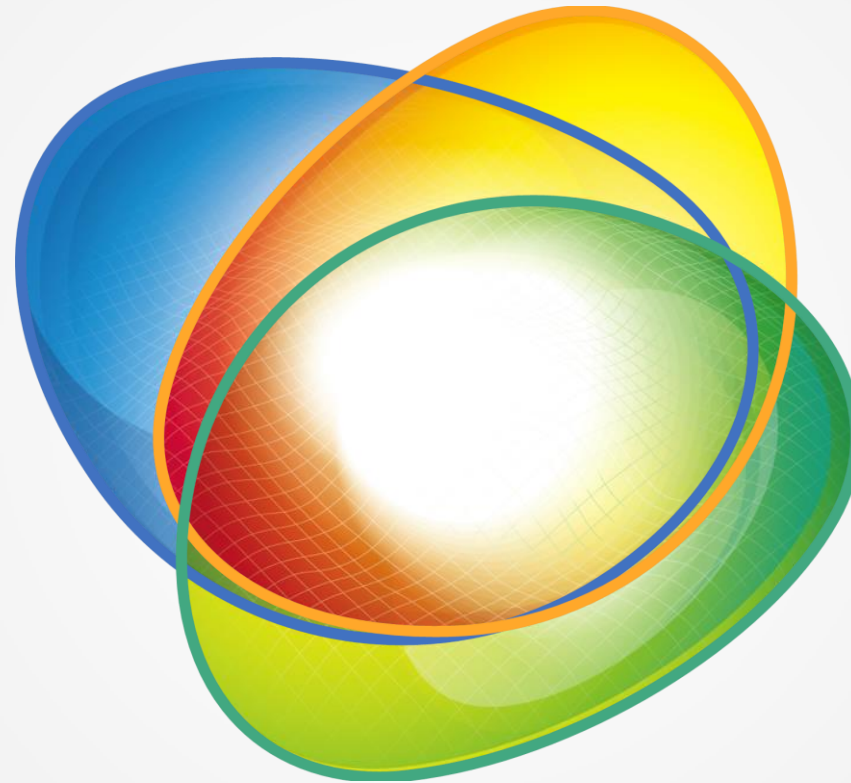
Extensible and
programmable

Anti-Fraud
Programmability
WAF
SSL intelligence
DNSSEC
Anti-Phishing
DDoS
ADF
SSL VPN
DNS Security
SSL Inspection



Software Defined Application Services Elements

Intelligent
Services Orchestration

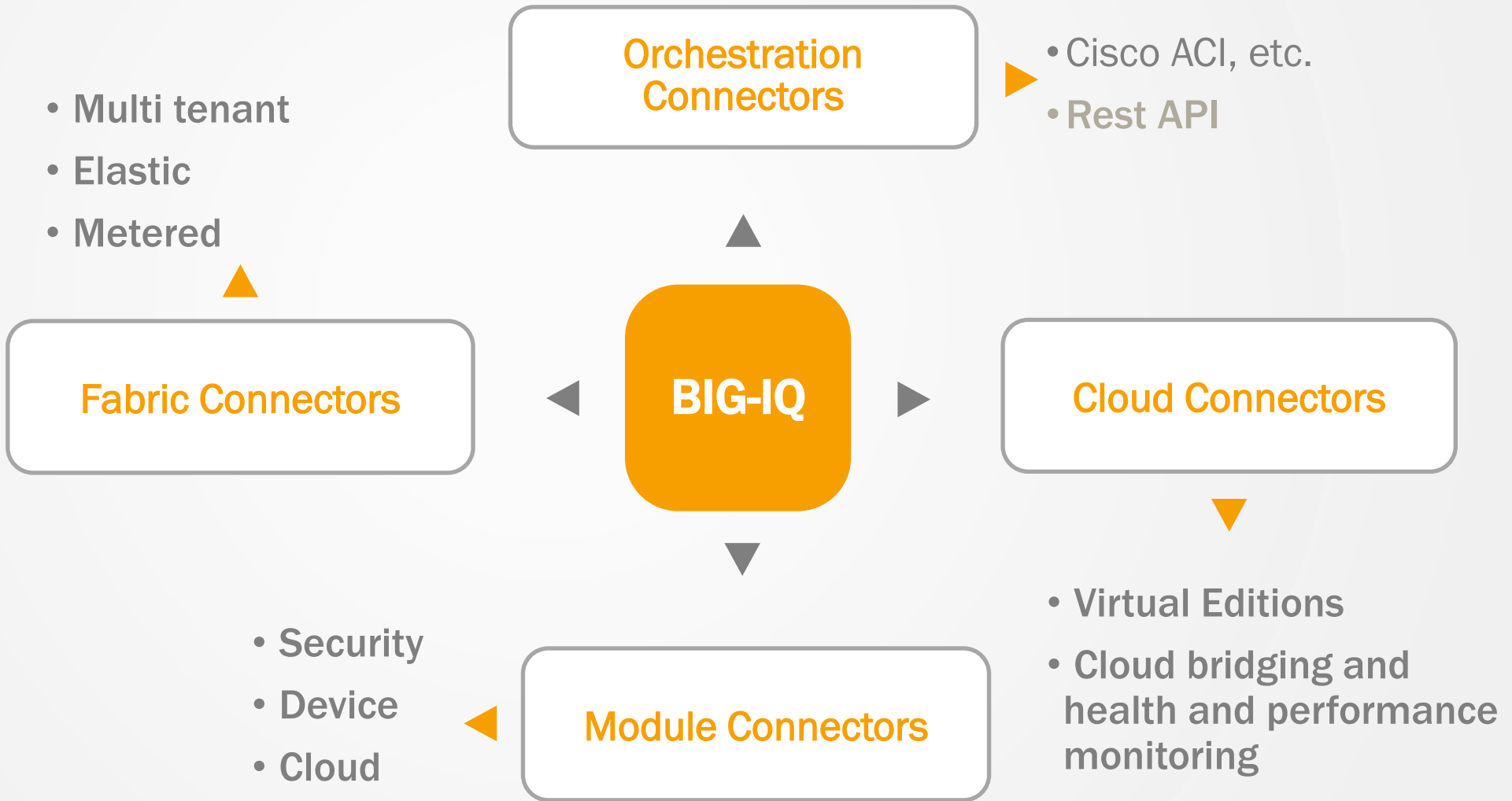


Intelligent Services Orchestration

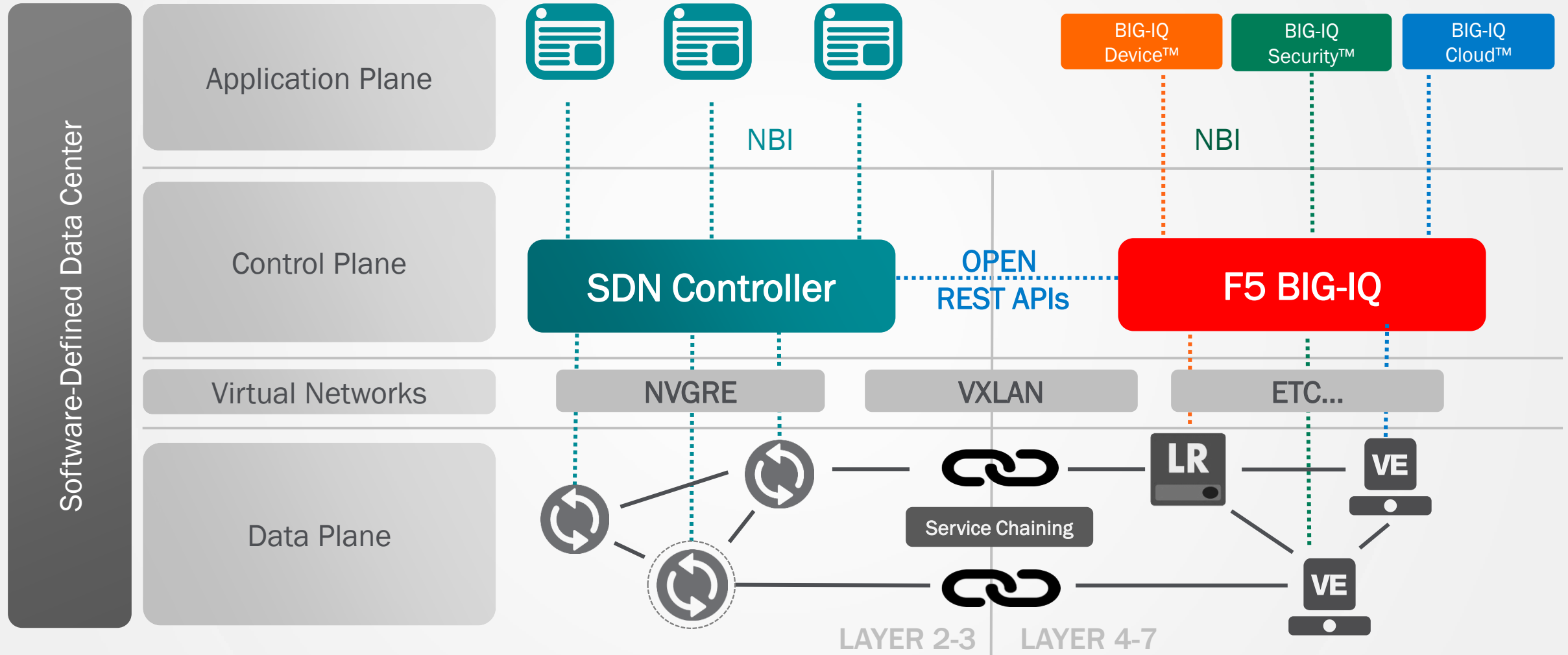
Single pane
of glass

Rapid system and
service provisioning

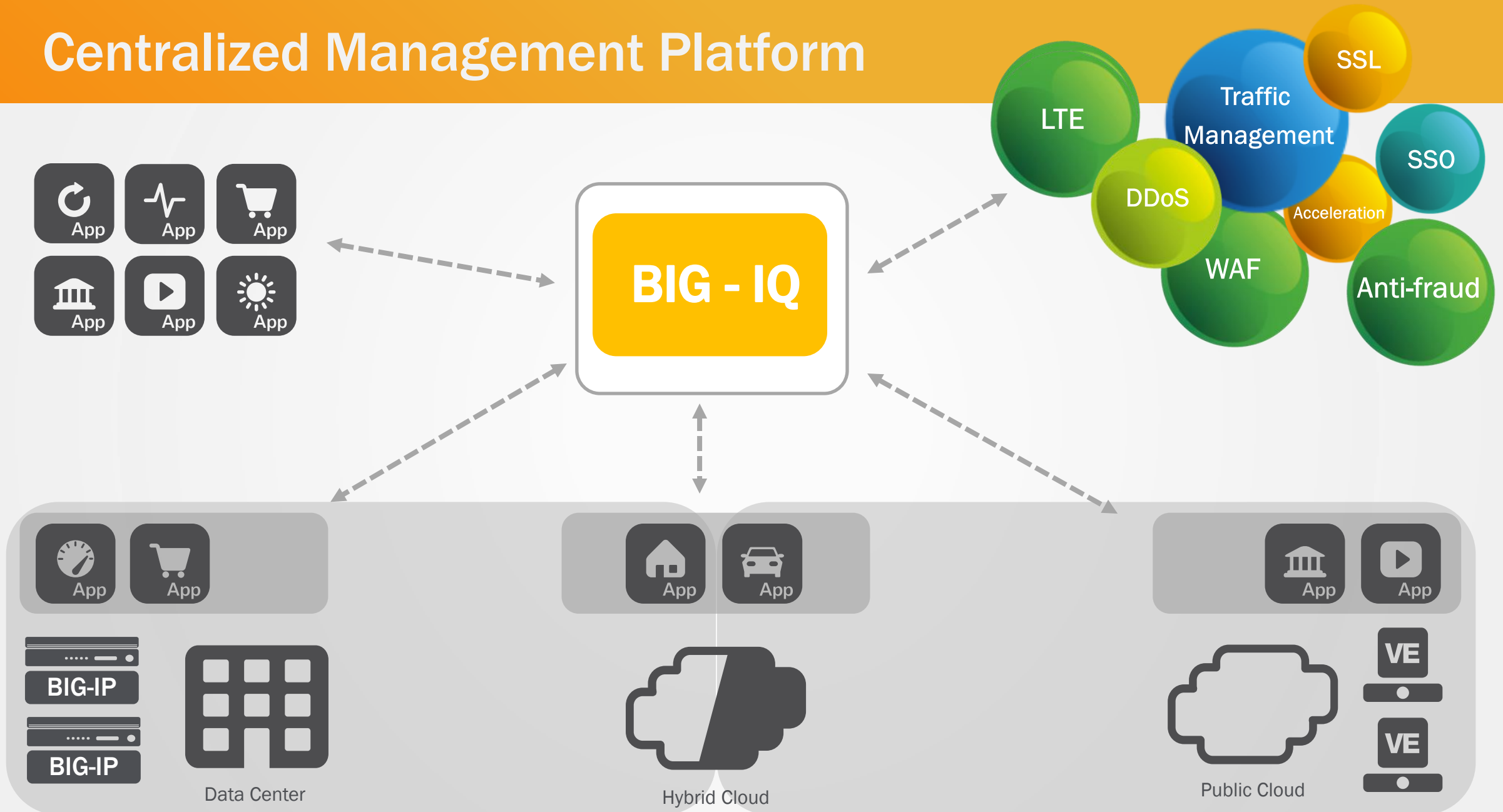
Ecosystem
enablement



Completing the SDN Stack



Centralized Management Platform



Application Services Modules

BIG-IQ Device



Cloud



BIG-IQ Security
Lifecycle Management
Lifecycle Management
Network Configuration

Develop

BIG-IQ Cloud



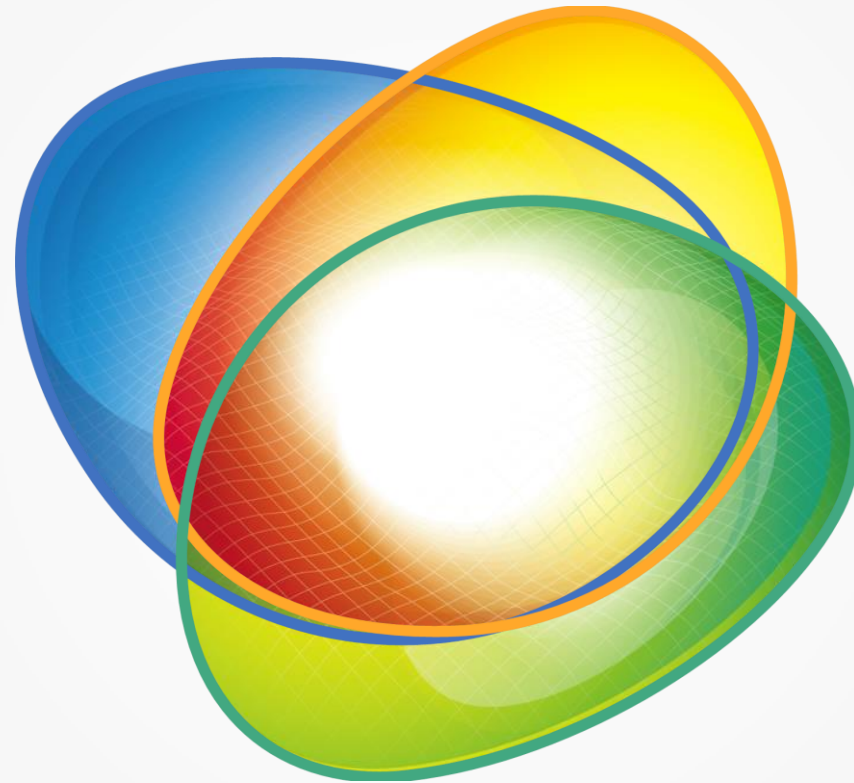
- Management fabric orchestration
- Public cloud connectors
- Application elasticity
- ADC self service management

BIG-IQ Security



- Policy based application security management
- Policy and rule monitoring
- Multi-tenant and multiuser editing and workflows

Software Defined Application Services Elements

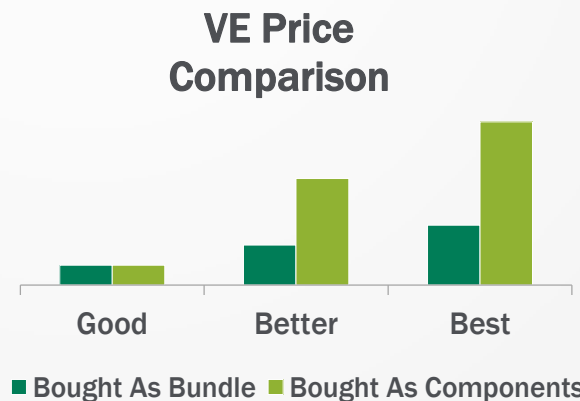
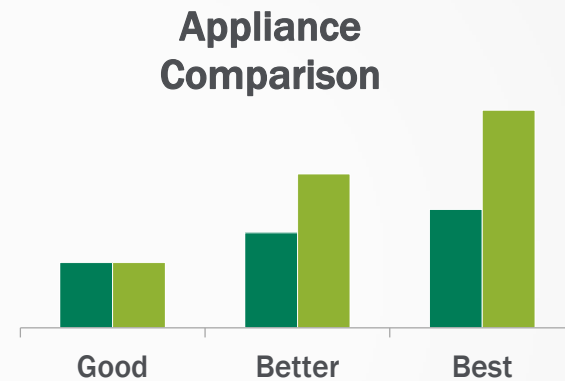


Simplified
Business Models

Good | Better | Best

Delivering Greater Customer Value

GBB Capabilities			
Modules/Services	Good	Better	Best
BIG-IP Local Traffic Manager	✓	✓	✓
BIG-IP Global Traffic Manager		✓	✓
Application Acceleration Manager		✓	✓
BIG-IP Application Protection		✓	✓
SDN Service		✓	✓
Advanced Routing		✓	✓
BIG-IP Access Policy Manager			✓
BIG-IP Application Security Manager			✓



Benefits

Flexibility	Make it easier to adopt advanced F5 functionality
Simplicity	Consolidate into fewer common configurations
Best Value	Save when purchasing bundles

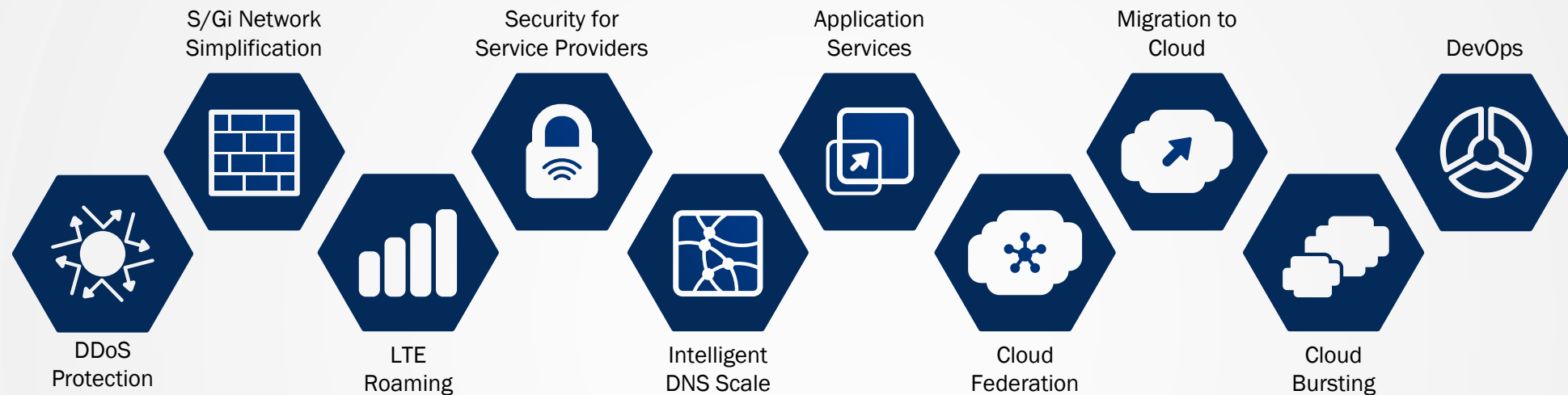
Reference Architectures

For Today's Customer Challenges



Reference Architectures

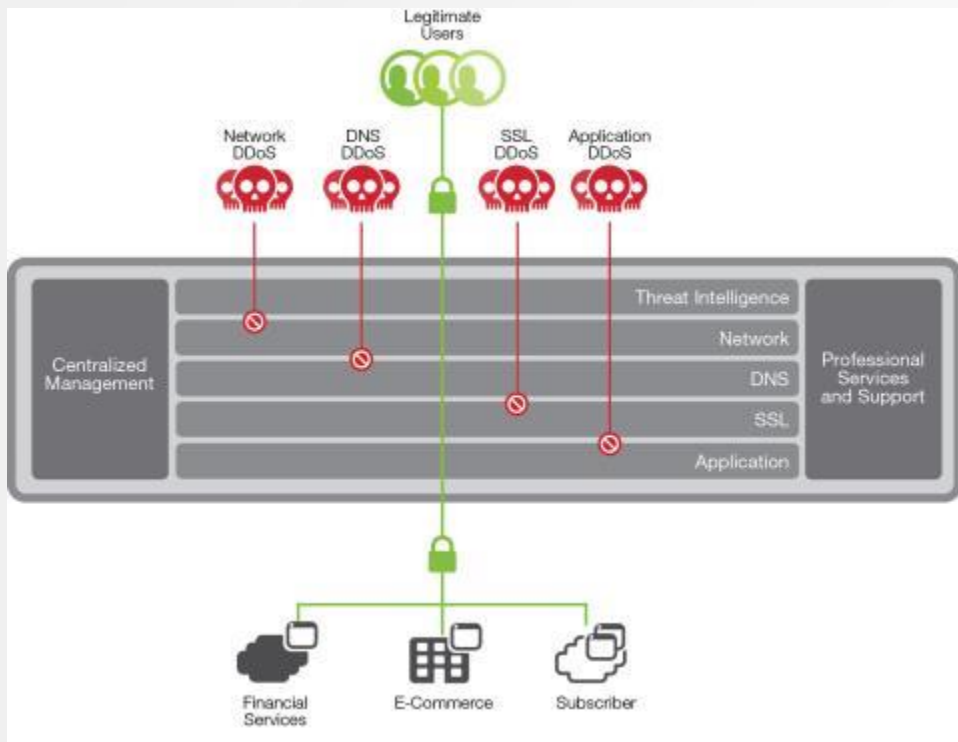
Device, Network, Applications



Bill of Materials

- White Paper (Business)
- Solution diagram(s)
- Architecture diagram(s)
- Product map diagram(s)
- Customer Presentation
- Solution Animation/Video
- White paper (Technical)
- Placemat leave-behind

Reference Architectures



The F5 DDoS Protection Reference Architecture

F5 offers guidance to security and network architects in designing, deploying, and managing architecture to protect against increasingly sophisticated, application-layer DDoS attacks.

White Paper

10 STEPS to Mitigate a DDoS Attack in Real Time

To the uninitiated, a DDoS attack can be a scary, stressful ordeal. But don't panic. Follow these steps to maximize success in fighting an attack.

- Verify that there is an attack**
Rule out common causes of an outage, such as DNS misconfigurations, upstream routing issues, and botnet size.
- Contact your team leads**
Gather the operations and applications team leads to verify what areas are being attacked and to already confirm the attack. Make sure everyone agrees on what areas are affected.
- Triage your applications**
Make triage decisions to keep your high-value apps alive. When you're under an internet DDoS attack and you have limited resources, focus on protecting revenue generators.
- Protect remote users**
Keep your business running. Whitelist the IP addresses of trusted remote users that require access, and maintain this list. Disable the list throughout the network and with service providers as needed.
- Classify the attack**
What type of attack is it? Volumetric? Slow and low? Your service provider will tell you if the attack is truly volumetric and may already have taken remediation steps.
- Evaluate source address mitigation options**
For advanced attack vectors your service provider can't mitigate, determine the number of sources. Block small lists of attacking IP addresses at your firewall. Block larger attacks with geolocation.
- Mitigate application layer attacks**
Identify the malicious traffic and whether it's generated by a known attack tool. Specific application layer attacks can be mitigated on a case-by-case basis with distinct countermeasures, which may be provided by your existing solutions.
- Leverage your security perimeter**
Did engineering issues? You could be performing an asymmetric layer 7 DDoS flood. Focus on your application-level defenses: login walls, human detection, or Full Browser Enforcement.
- Constrain resources**
If previous steps fail, simply constraining resources, like rate and connection limit, is a last resort—it can take away both good and bad traffic. Instead, you may want to disable or throttle an application.
- Manage public relations**
If the attack becomes public, prepare a statement and notify internal staff. If industry partners allow it, be forthright and admit you're being attacked. First, cite technical challenges and advise staff to direct all inquiries to the PR manager.

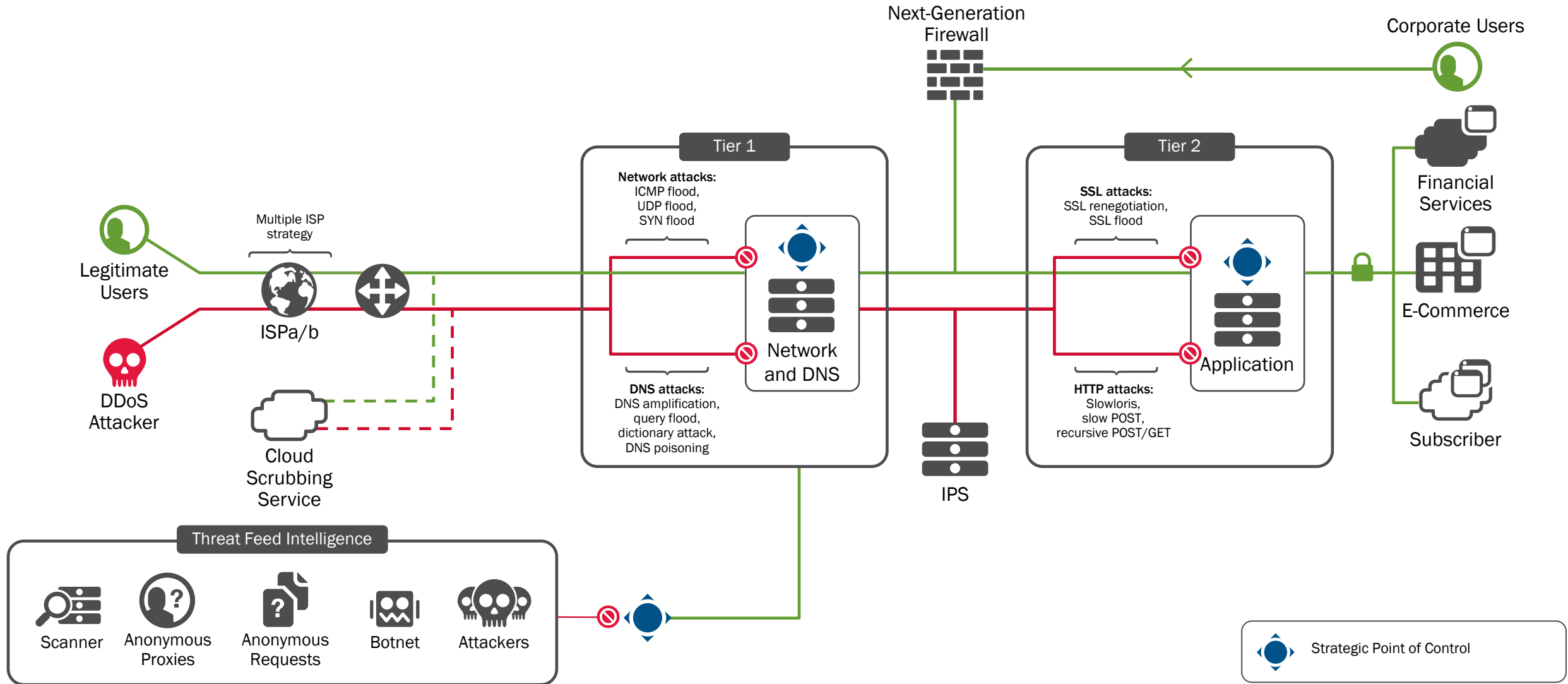
Take the next step

You've mitigated today's attack. Now focus on building the right DDoS protection architecture for your business.

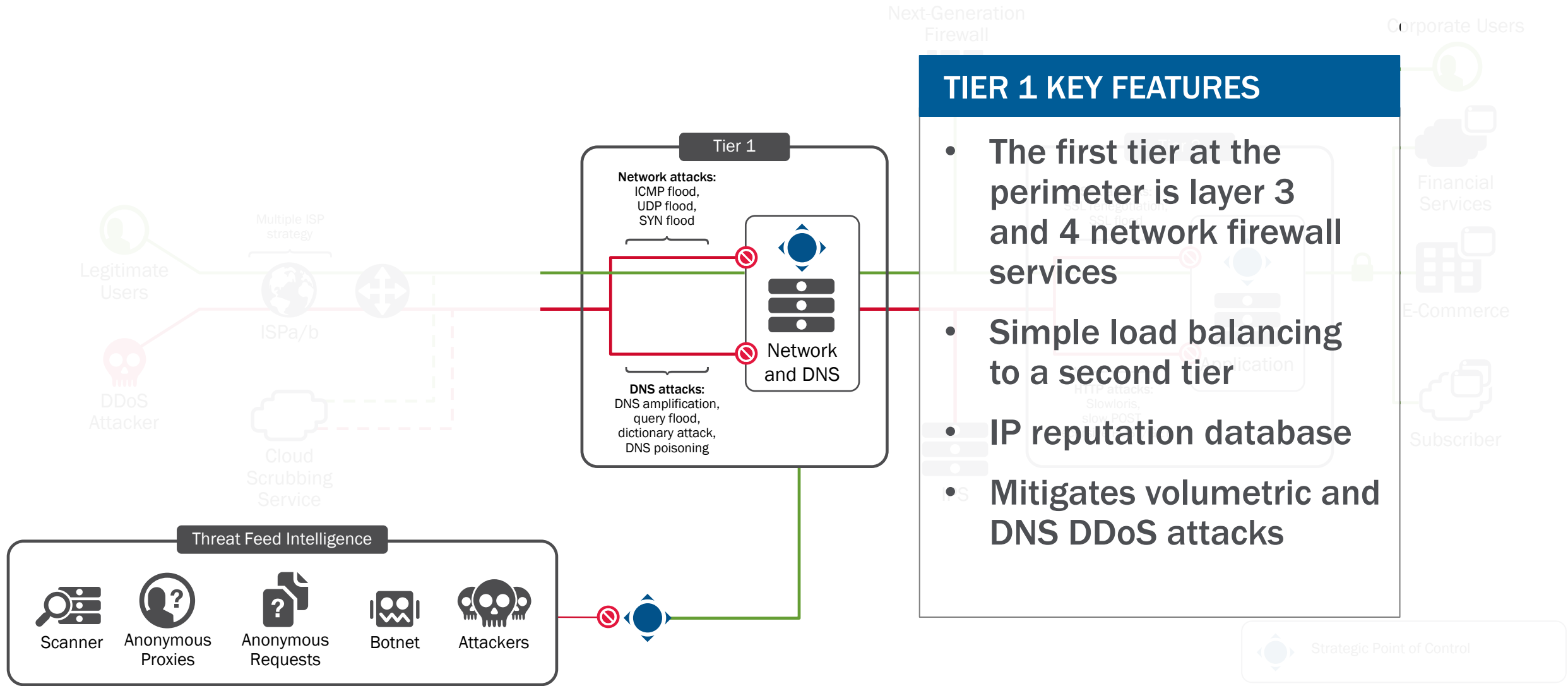
f5 f5.com

Solution Documents...

DDoS Protection Reference Architecture



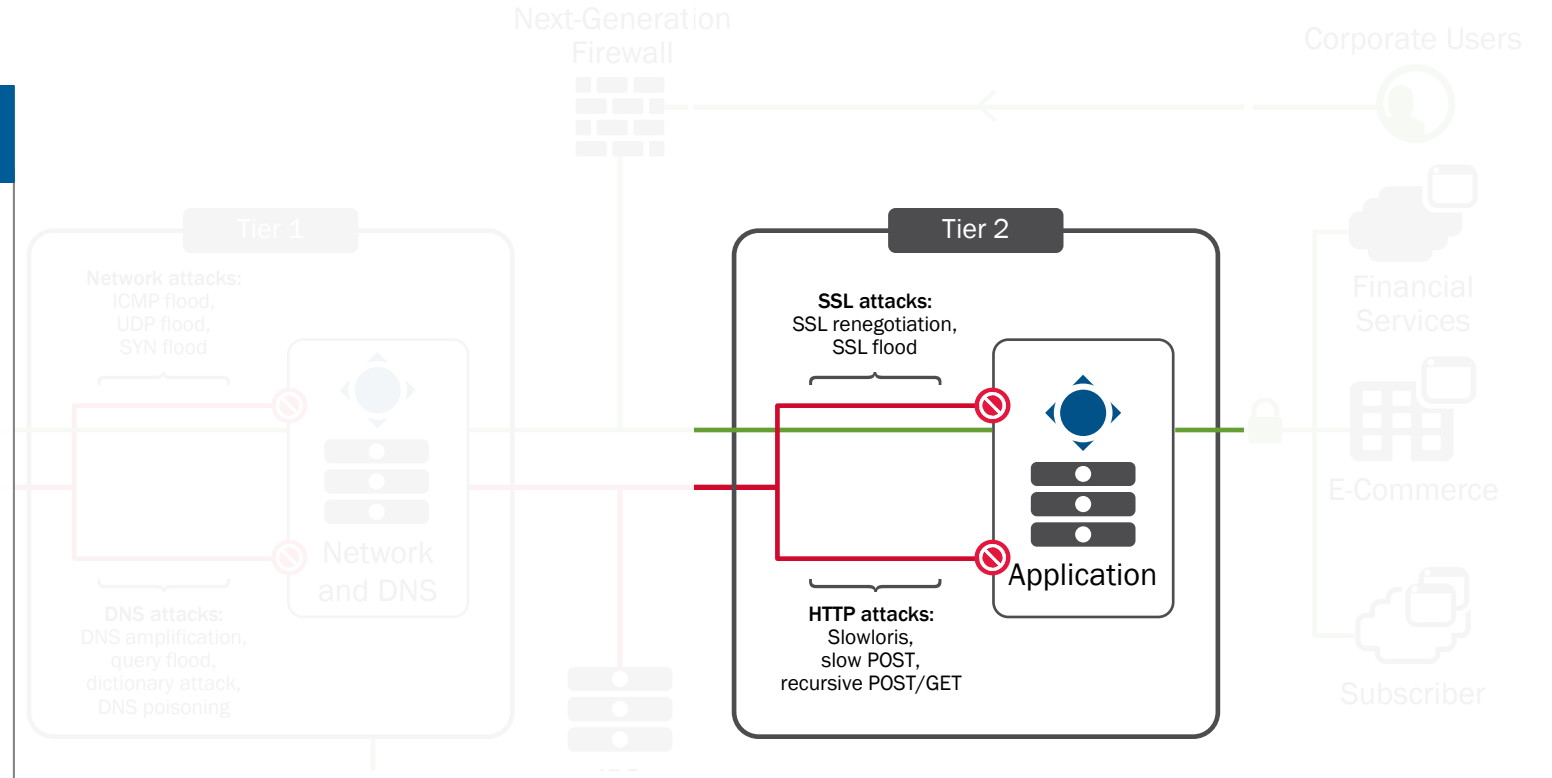
DDoS Protection Reference Architecture



DDoS Protection Reference Architecture

TIER 2 KEY FEATURES

- The second tier is for application-aware, CPU-intensive defense mechanisms
- SSL termination
- Web application firewall
- Mitigate asymmetric and SSL-based DDoS attacks



Recommended Practices Configuration Guide

2.3.2.4 Enforce Real Browsers

Besides authentication and tps-based detection (section **Error! Reference source not found.**), there are additional ways that F5 devices can separate real web browsers from probable bots.

The easiest way, with ASM, is to create a DoS protection profile and turn on the “Source IP-Based Client Side Integrity Defense” option. This will inject a JavaScript redirect into the client stream and verify each connection the first time that source IP address is seen.

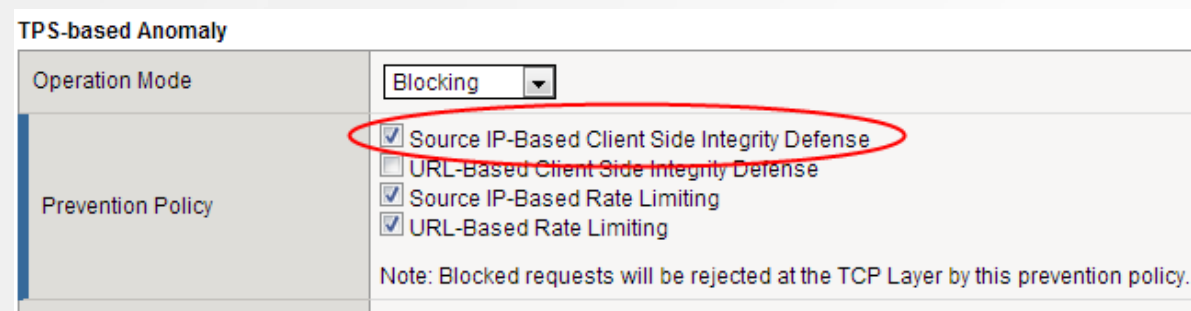


Figure 1. Insert a Javascript Redirect to verify a real browser

32 Page Detailed Guide...

2.3.2.5 Throttle GET Request Floods via Script

The F5 DevCentral community has developed several powerful iRules that automatically throttle GET requests. Customers are continually refining these to keep up with current attack techniques.

Here is one of the iRules that is simple enough to be represented in this document. The live version can be found at this DevCentral page: [HTTP-Request-Throttle](#)

```
when RULE_INIT {
    # Life timer of the subtable object. Defines how long this object exist in the subtable
    set static::maxRate 10
    # This defines how long is the sliding window to count the requests.
    # This example allows 10 requests in 3 seconds
    set static::windowSecs 3
    set static::timeout 30
}

when HTTP_REQUEST {
    if { [HTTP::method] eq "GET" } {
        set getCount [table key -count -subtable [IP::client_addr]]
        if { $getCount < $static::maxRate } {
            incr getCount 1
            table set -subtable [IP::client_addr] $getCount "ignore" $static::timeout $static::windowSecs
        } else {
            HTTP::respond 501 content "Request blockedExceeded requests/sec limit."

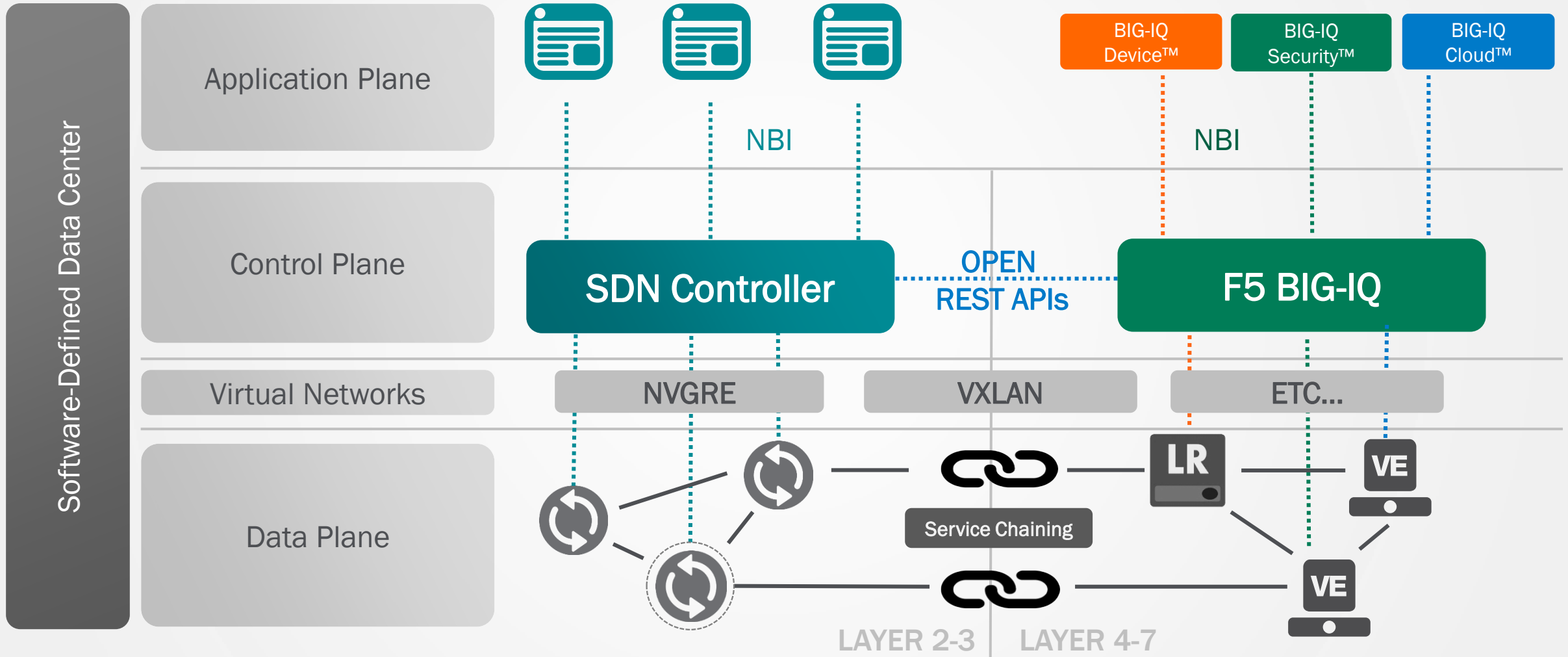
            return
        }
    }
}
```

Another iRule, which is in fact descended from the above, is an advanced version that also includes a way to manage the banned IPs address from within the iRule itself:

- [URI-Request Limiter iRule](#) – Drops excessive HTTP requests to specific URIs or from an IP

Cisco Partnership

Completing the SDN Stack



Partner Integration with Synthesis

Auto-scaling, application provisioning, and automated system maintenance and patching.

Two-way communication
Configure application networking services
Automated network and service provisioning

BIG IQ Cloud

Programmability

F5 SDAS Service Fabric

Programmability

F5 Platforms

Hardware | Software | Cloud

Integrate network virtualization and ADN services

 **amazon** | **EC2**
web services™

Provisioning and orchestration of BIG-IP in AWS


CISCO /
insjeme
NETWORKS

Automate network and service provisioning,

Cisco ACI Design Philosophy

ACI Design Philosophy: Six Fundamental Principles



1
Application Velocity.
Any Workload.
Anywhere.



2
Common Platform—
Integration of
Physical, Virtual,
and Cloud



3
Common Policy,
Management and
Operations
(Network, Security,
and Applications)



4
Systems
Approach



5
Open APIs,
Open Source,
Open Standards



6
Lowest Total
Cost of Ownership

Designed from the Ground-Up to be Application Centric

Why Cisco/ACI matters for Customers

- Cisco and F5 share a common vision for simplifying networking end to end by taking an application-centric approach to solving key pain points in customer's next generation data centers while meeting their critical data center requirements today.
- Working with Cisco on Application Centric Infrastructure, F5 has a unique opportunity to deliver on vision of shaping infrastructure to the needs of the applications.
- Cisco ACI integrates F5 Big-IP appliances (physical and virtual) to deliver application-centric, ADC-enabled network automation in existing and next generation data centers

Benefits

Drive Business Value

- Improve application availability, reliability, recoverability, performance, security, and velocity

Increase IT Capabilities

- Common platform physical | virtual | cloud
- Moving from managing devices to services

Reduce Costs

- Lower TCO
- Consolidate user, network, and application services

Future Proof

- Programmability and orchestration
- Open APIs, open standards
- Application awareness

Growth Opportunities



Security



SDDC/Cloud

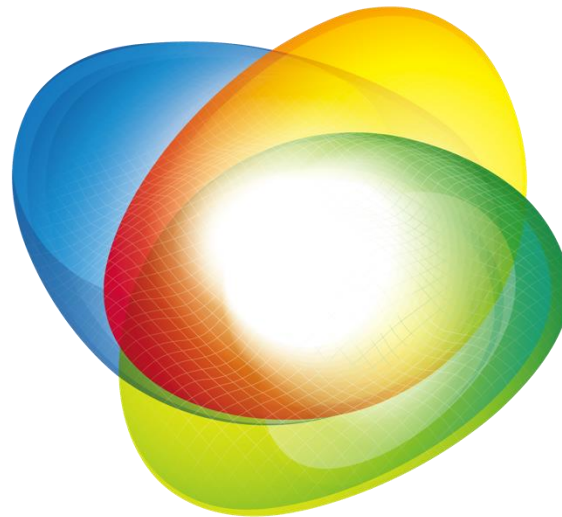


Mobility

Reference Architectures



f5 Synthesis™





devcentral.f5.com

facebook.com/f5networksinc

linkedin.com/companies/f5-networks

twitter.com/f5networks

youtube.com/f5networksinc

synthesis.f5.com