



Hybrid DDOS Mitigation

Yasser Elmashad

Gad Elkin

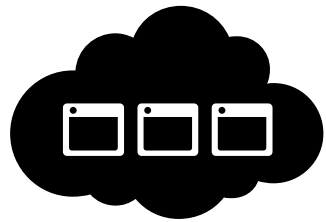


DDOS Scene



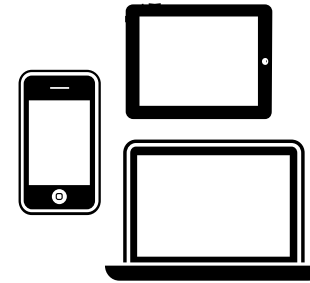
Protecting Against DDoS is Challenging

Webification of apps



71% of internet experts predict most people will do work via web or mobile by 2020

Device proliferation



95% of workers use at least one personal device for work

130 million enterprises will use mobile apps by 2014

Evolving security threats

58% of all e-theft tied to activist groups

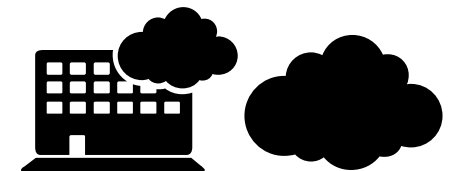
81% of breaches involved hacking



Shifting perimeter

80% of new apps will target the cloud.

72% of IT leaders have or will move applications to the cloud



The evolution of attackers

September 1996

First high profile DDoS attack. NY ISP Panix.com that was nearly put out of business.

January 2008

Anonymous executes a series of high-profile DDoS attacks against the Church of Scientology.

December 2010

WikiLeaks supporters hit PayPal, Visa, Mastercard, and other financial sites with DDoS attacks.

April 2011

Attackers use a DDoS attack against Sony to mask the theft of millions of customer records.

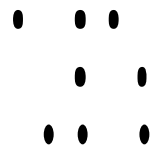
April 2012

Anonymous knocks down the sites of the U.S. Dept. of Justice, the CIA, and the British Secret Intelligence Service.

September 2012

Syrian Cyber Fighters launch Operation Ababil with DDoS attacks on 13 U.S. banks to protest an anti-Muslim video.

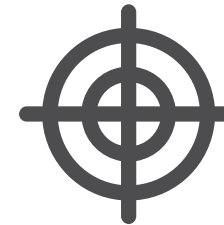
1996 | ... | 2008 | 2009 | 2010 | 2011 | 2012 | 2013



**Script
kiddies**



**The rise
of hacktivism**



**Cyber
war**

The evolution of attackers

December 2014

Lizard Squad strikes XBOX and Play Station Network.

March 2015

Massive github DDoS attack tied to Chinese government.

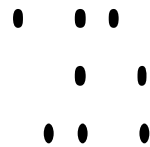
January 2016

BBC sites targeted with the largest DDoS attack in history by the group New World Hacking using the BangStresser DDoS tool.

2014

2015

2016



**Script
kiddies**



**The rise
of hacktivism**



**Cyber
war**

The business impact of DDoS



**The business impact
of DDoS**



**Cost of
corrective action**



**Reputation
management**

DDOS is a business

How to attack someone?

Do it yourself approach

Tons of videos available on how to DDOS someone

Need to rent / use botnets : <10\$ an hour, <300\$ a day for 1000 hosts

Become a member of an hacktivist group
They can provide you the DDOS tools like LOIC:

DDOS as a service

Buy in 2 clicks for less than 20 €/month 14 Gbps of attack...

<http://down-api.eu/#>

Vendor pckabml Price ₮0.00244696 Location United Kingdom

 **ddos attack**

hansamkt2rr6nfg3.onion/listing/303 Hansa Market

i will ddos any website indefinatley i run a large scale botnet hosted on 5 servers with high bandwidth

Vendor jesse Price ₮0.068698 Location Worldwide

rent ddos - Grams Valhalla

valhallaxmn3fydu.onion/products/9532

valhallaxmn3fydu.onion Suomeksi Register Log in

You can browse products and vendors without logging in. For making purchases you'll need to **register an account**.

ATHENA BOTNET 1.08 PANEL + BUILDER

4.54 EUR (0.012062 BTC)
more than 25 pcs in stock
Paper500 (0)
Finland → Finland

JavaLOIC

Low Orbit Ion Cannon

1. Select target
Host 192.168.1.1
URL
Selected target: 192.168.1.1

2. Attack options
Timeout 9'000 HTTP Subsite Random TCP/UDP Message Random
Port 80 Method Threads Wait for reply 30 Delay (ms)
Socks proxy 127.0.0.1 Port 8'080

Attack status
Running Requested 98 Fails 10

Praetox.com

Once they were only a few, now attackers are coming out in record numbers



Attack Threats: Pay up or Else!

Emails sent to legitimate businesses with the threat of massive DDoS attacks

Right now we are running small demonstrative attack on 1 of your IP's

Don't worry, it will not be that hard and it will stop in 1 hour.
It's just to prove that we are serious.

We are aware that you probably don't have 25 BTC at the moment, so we are giving you 24 hours.

Find the best exchanger for you on

DD4BC | Armada Collective | Caremini | Wh0Ami76 | Wh0Ami78

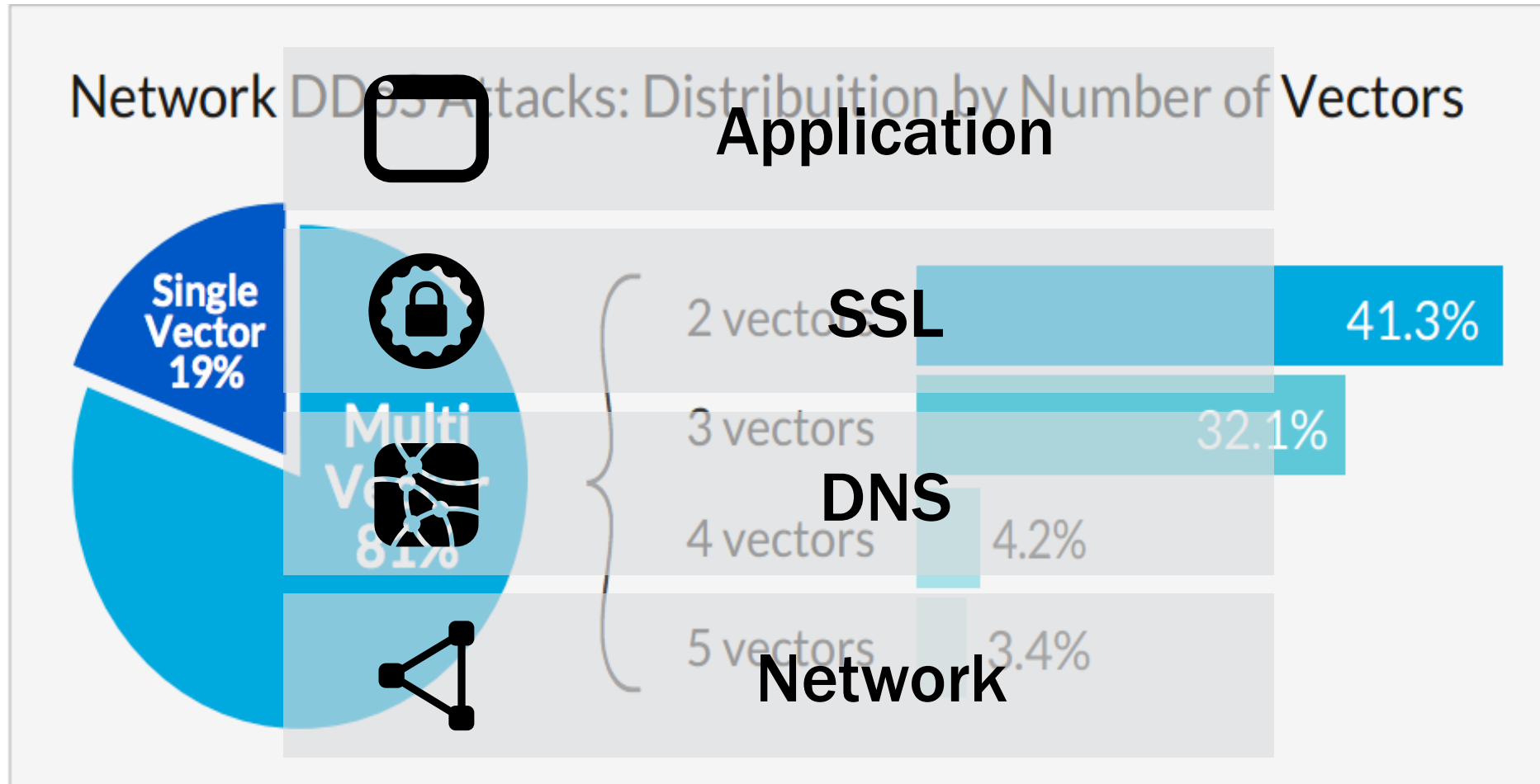
You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet.

Current price of 1 BTC is about 230 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don't even have to reply. Just pay 25 BTC to 155JPhzJmLBNqk12xaGRoDcNkAXNbmegjj – we will know it's you and you will never hear from us again.

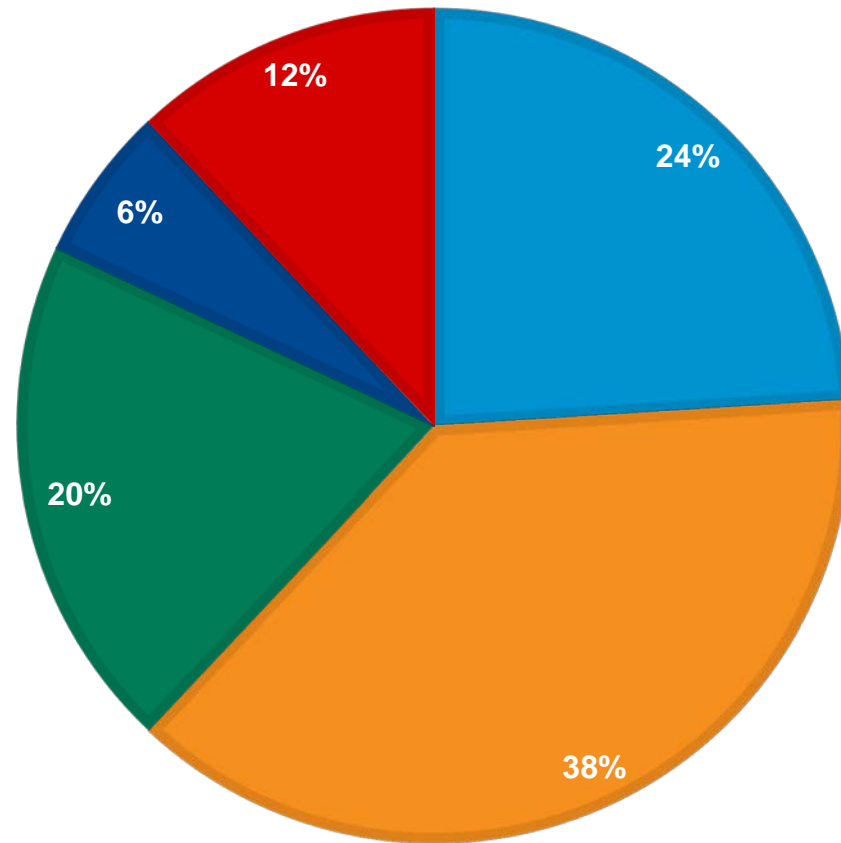
We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated. If you need to contact us, feel free to use some free email service. Or contact us via Bitmessage: BM-NC1jRwNdHxX3jHrufjxDsRWXGdNisY5

More sophisticated attacks are multi-Layer



Attack Size

■ 0.5-1 Gbps ■ 1-10 Gbps ■ 10-50 Gbps ■ Over 50Gbps ■ Unknown



Hybrid Concept



Gartner on DDoS – Go Hybrid!

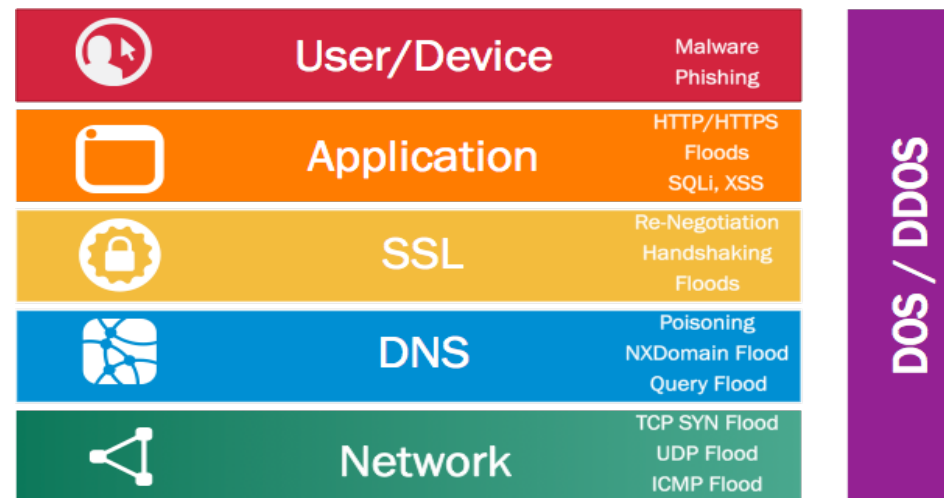
- Ensure That Business Continuity / Disaster Recovery and Incident Response Plan Address Planning-for and Response-to DDoS
- Evaluate ISP “Clean Pipe” Services
- Evaluate DDoS “Mitigation as a Service” Options
- Deploy DDoS Detection and Mitigation Equipment on Premises

Hybrid DDoS Protection:

“Cloud + On-Premise” Makes the most sense



Hybrid Security platform that provides full proxy architecture to fill L3-L7 security gap holistically.

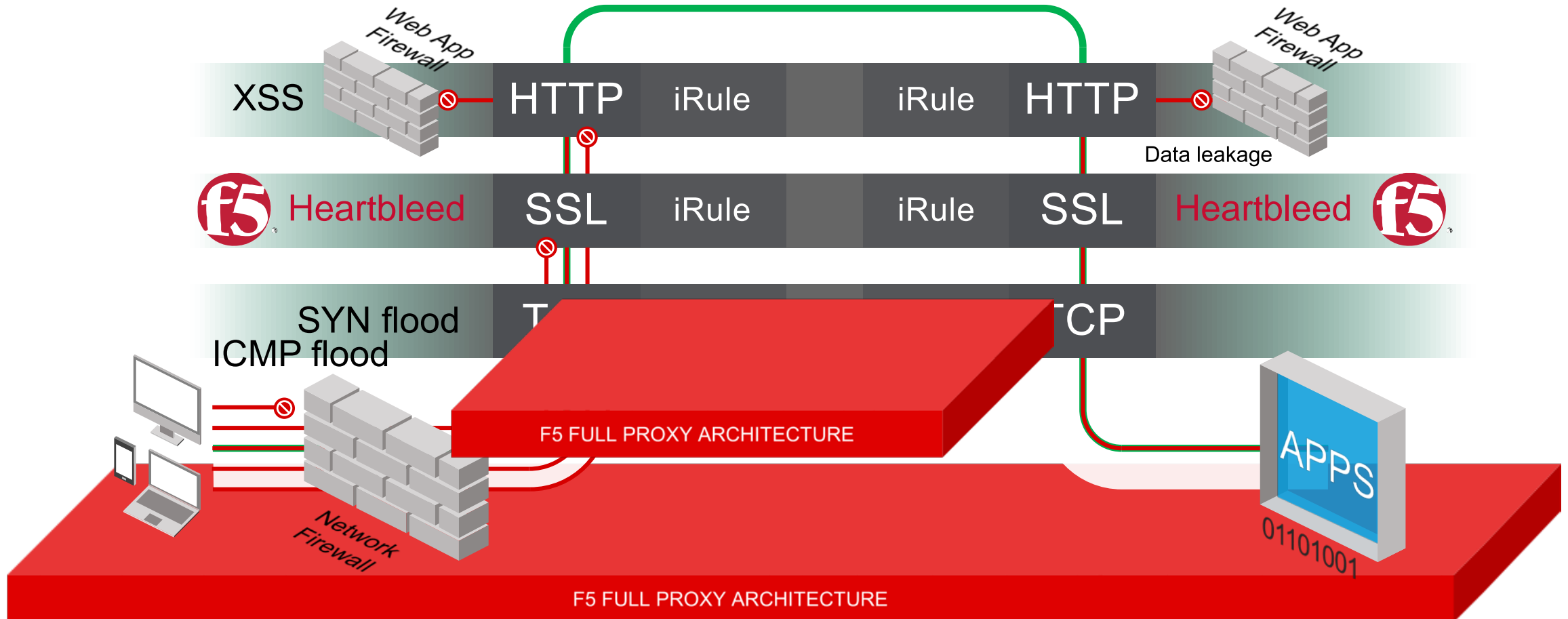


F5 DDoS On Premises

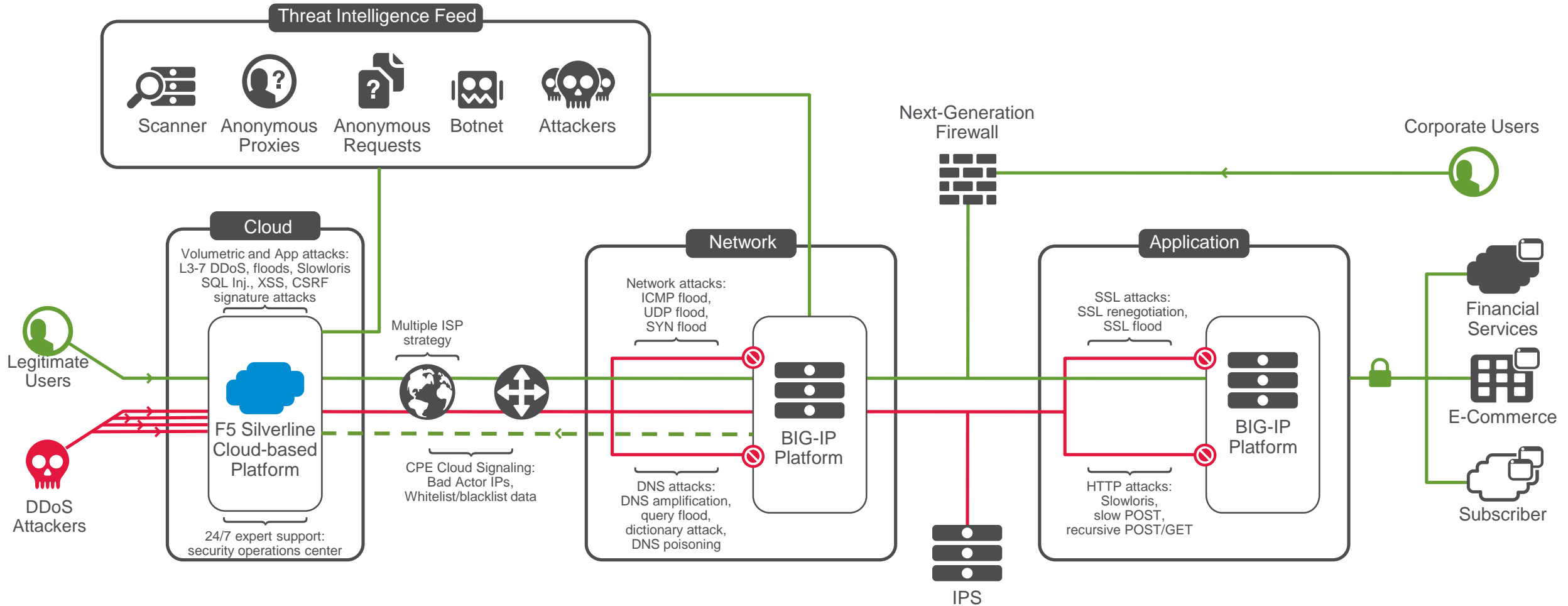


Full Proxy Architecture

Block client and server-side attacks that target Open SSL vulnerabilities



Comprehensive DDoS Protection



Layer 7 HTTP/S DoS attack protection

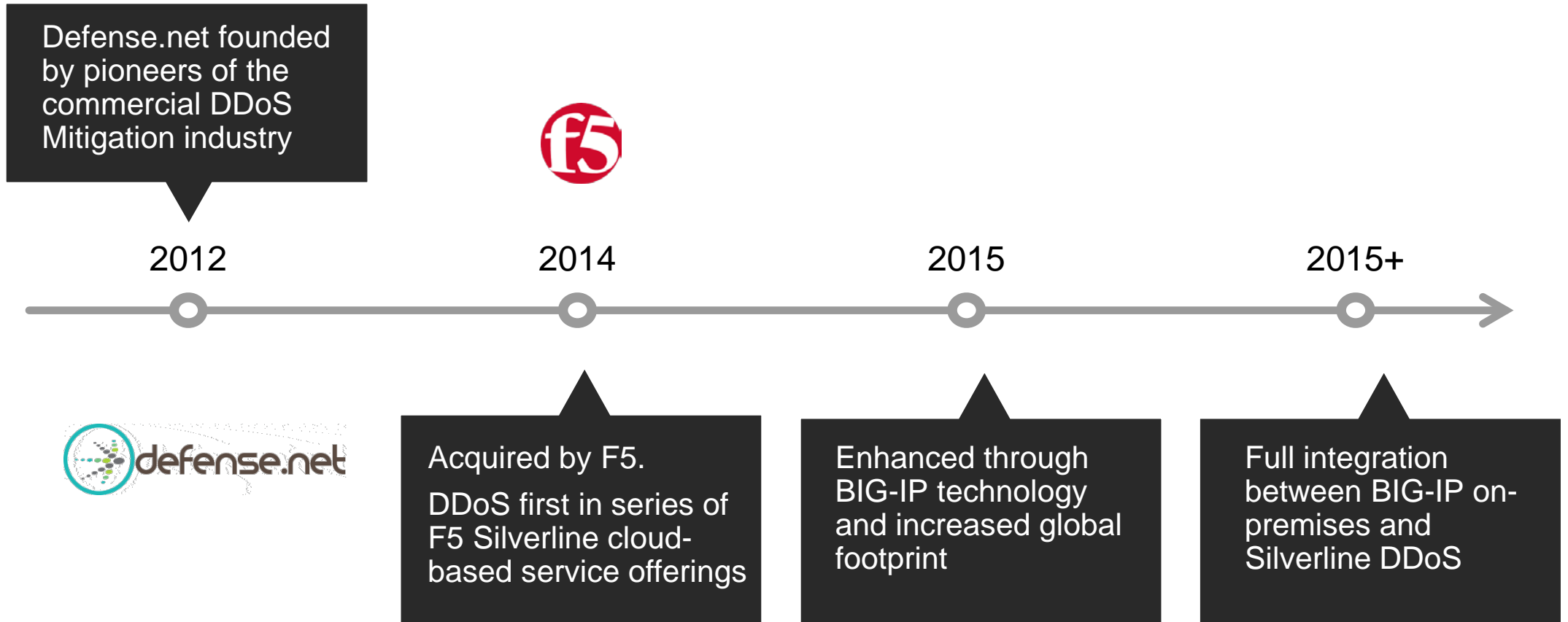
- Guards against RPS (TPS) and latency-based anomalies
- Provides predictive indicators
- Support IP, geolocation, URL and site wide detection criteria
- Provides heavy URL protection
- Protects against threats proactively
- Simplified reports access and added qkView violations export support
 - **Advanced Prevention techniques**
 - Client Side Integrity Defense
 - CAPTCHA (HTML or JS response)
 - Source IP Blocking
 - Geolocation blacklisting



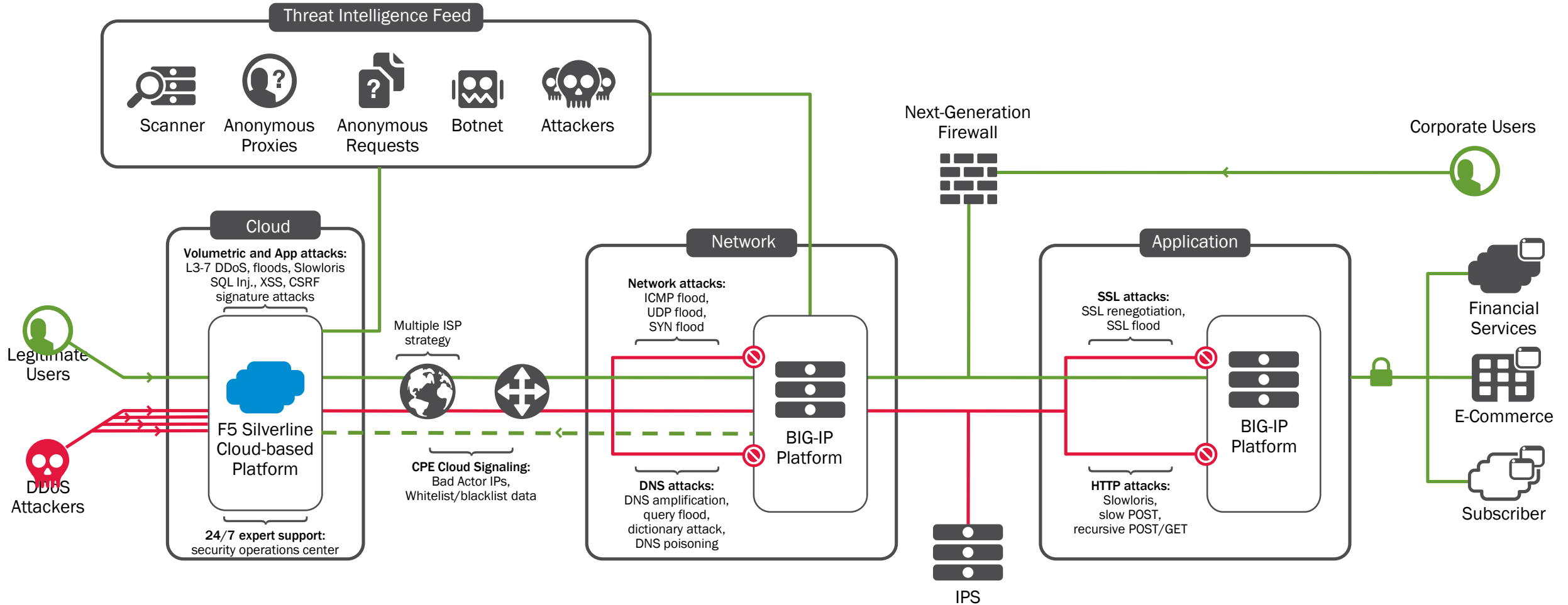
F5 DDoS Managed Service



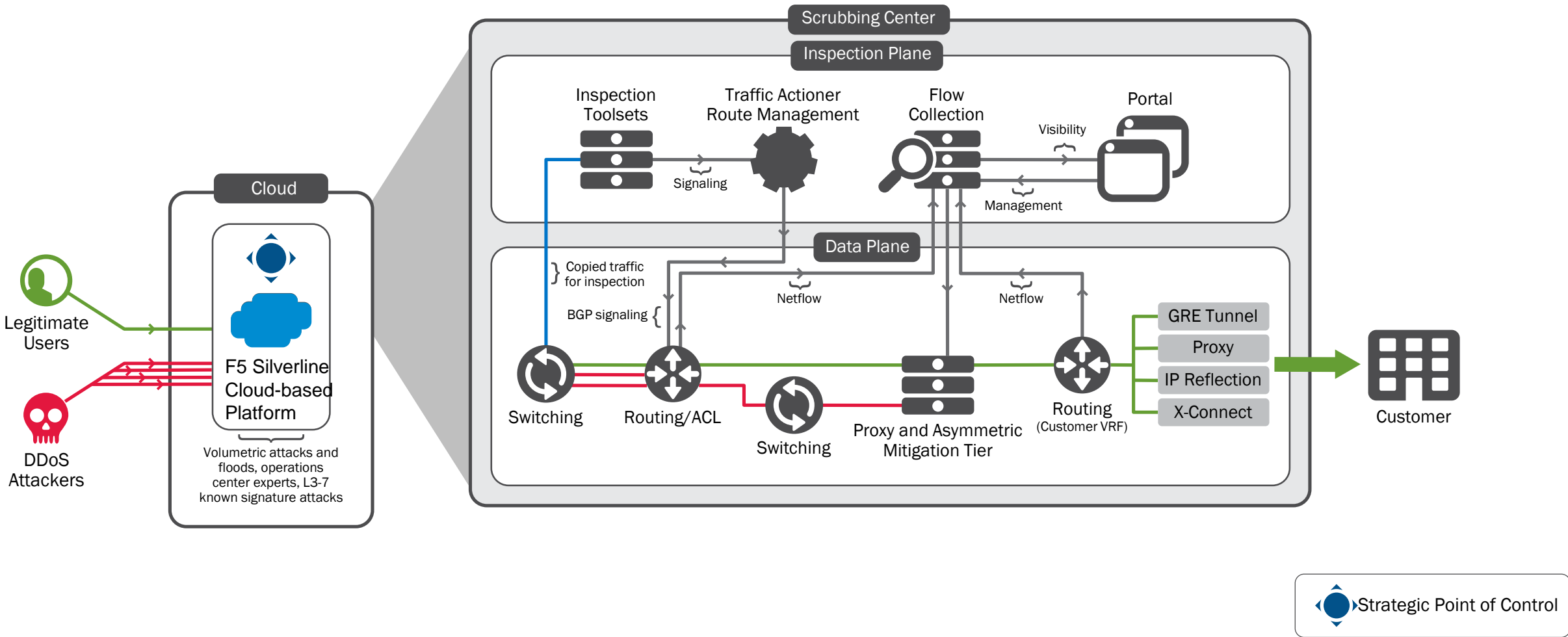
The Silverline DDoS protection story



Silverline DDoS Protection



DDoS Architecture Scrubbing Center



Global Coverage



24/7 Support

F5 Security Operations Center (SOC) in Seattle: staffed 24x7x365 with security experts for DDoS Protection and WAF. Warsaw is staffed for Websafe.

- Seattle, WA U.S.
- Warsaw, Poland

Global Coverage

Fully redundant and globally distributed data centers world wide in each geographic region

- San Jose, CA US
- Ashburn, VA US
- Frankfurt, DE
- Singapore, SG

Industry-Leading Bandwidth

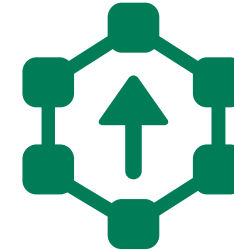
- Attack mitigation bandwidth capacity over 1.0 Tbps
- Scrubbing capacity up to 1.0 Tbps (with upstream ACLs)
- Guaranteed bandwidth with Tier 1 carriers

F5 Silverline - Service Options



Always On

Primary protection as
the
first line of defense



Always Available

Primary protection
available on-demand

Traffic Steering to SL

VS

Capabilities

BGP (BORDER GATEWAY
PROTOCOL)
ROUTED MODE

DNS
PROXY MODE

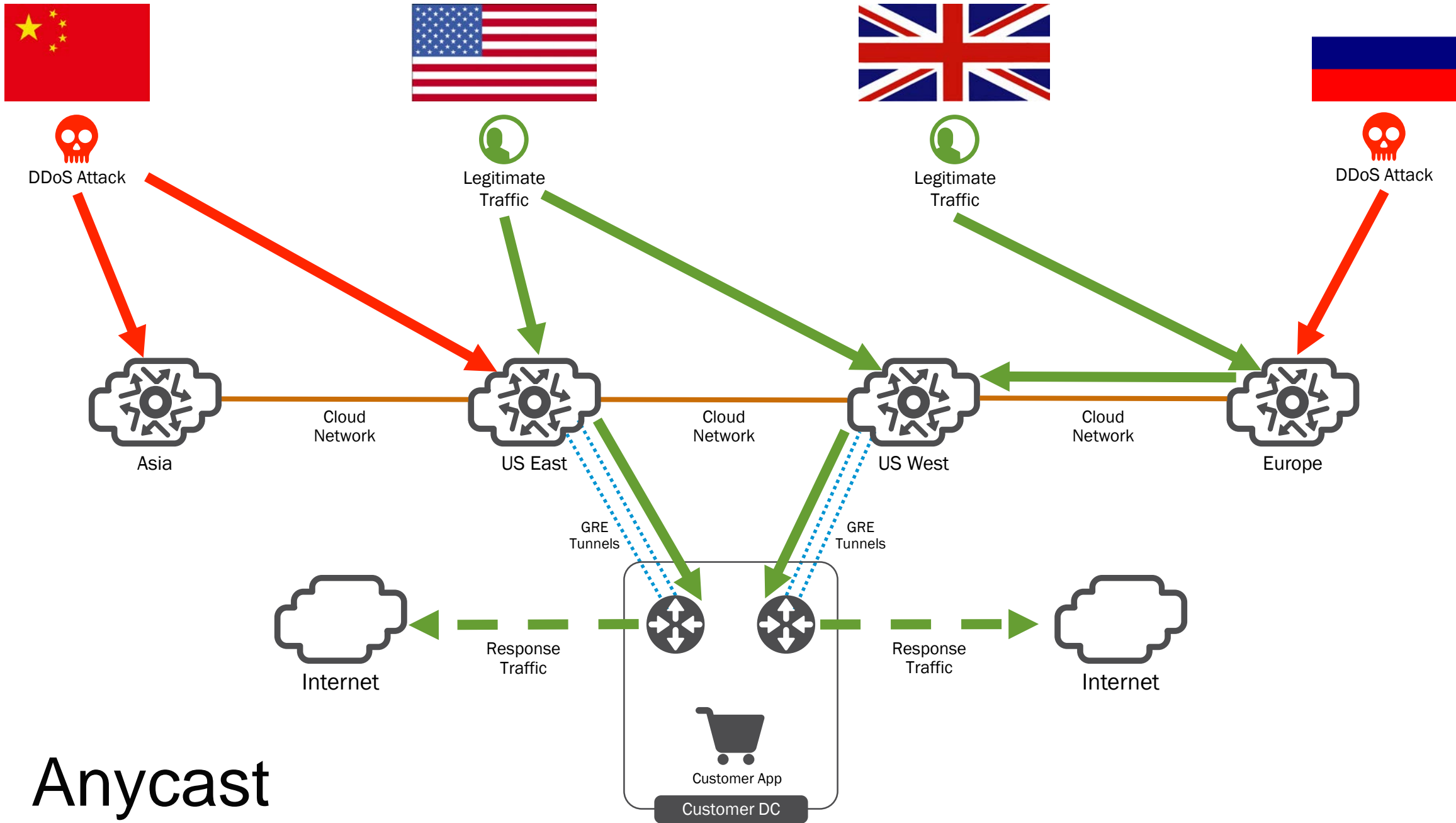
PROTECT ENTIRE NETBLOCK /24

ASYMETRIC L3/L4

TUNNEL CLEAN TRAFFIC

SINGLE APPLICATION (IP)

FULL PROXY
L7
SSL TERMINATION
WAF



Anycast

Gain attack insights and intelligence

F5 Customer Portal

Securely communicate with Silverline
SOC experts

View centralized attack and threat
monitoring reports with details including:

source geo-IP mapping

blocked vs. alerted attacks

blocked traffic and attack types

alerted attack types

Threats*

bandwidth used

hits/sec*

type of traffic and visits (bots v. humans)*



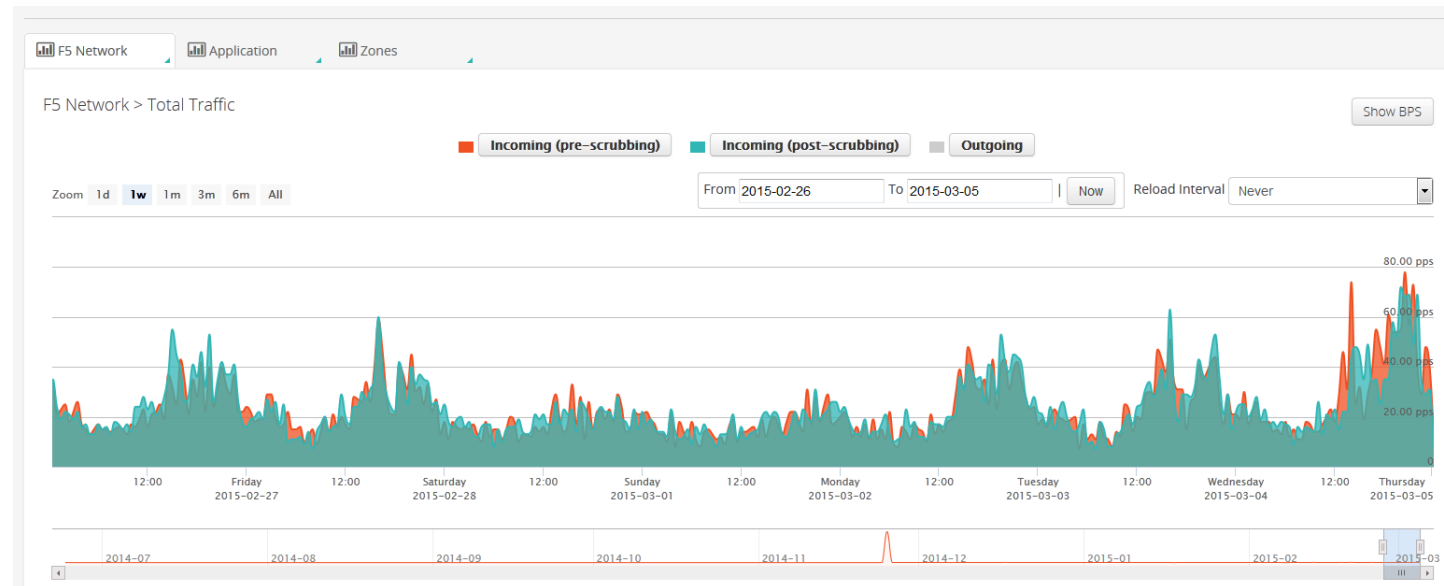
Customer Portal



Visibility &
Compliance



Attack Reports



Security Operations Center

Outsourcing DDoS Monitoring and Mitigation



Monitoring and mitigating attacks while reducing false positives requires a 24/7 staff of skilled DDoS analysts

- Full provisioning and configuration
- Proactive alert monitoring
- Identification and inspection of attacks
- Custom and script mitigation

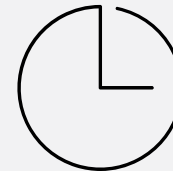
Service level agreements time to:

- Notify, mitigate, escalate

Security Operations Center (SOC)



Tier II DDoS
Analysts and Above



Availability
and Support



Active DDoS
Threat Monitoring

F5 Hybrid Security



Hybrid Security with F5

**Anti-DDoS
Managed Service**

**Web Application
Firewall
Managed Service**

F5 Silverline Cloud Security

High Performance Security

Simplified Security

Scalable Security

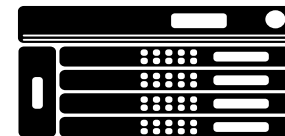
BIG-IP Platform on-premises



Virtual Edition



Appliance



Chassis

Rethink.....Multi-Layer Security with F5

DDoS
Protection

App
Protection

Network
Protection

Web
Fraud
Protection

SSL
Visibility &
Protection

DNS
Protection

App
Access

TMOS - Full Proxy

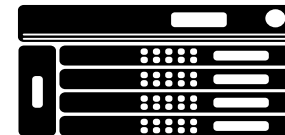
BIG-IP Platform



Virtual Edition



Appliance



Chassis

Key DDoS Mitigation Values

Protection



Protect against the full spectrum of modern cyber threats attacks

100+ DDoS Vectors;
Most advanced app security; 98% of fortune 1000 trust their traffic to F5

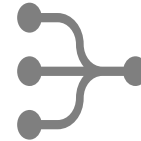
Performance



Minimize business impact from volumetric attacks 7.5M

Up to 640 Gbps;
7.5M CPS; 576M CCS; in the datacenter and over 1Tbps in the cloud

Extensibility



Take immediate action on new DDoS threats

1,000's of iRules have been written to mitigate traffic based on any type of content data

Expertise



Augment resources with F5 Security experts

24x7x365 DDoS support from Security Operations Centers in the US, APAC, and EMEA

F5 Emergency Response Service

**UNDER DDoS
ATTACK?**


Get back to business with
F5 Silverline DDoS Protection.



CALL
00-800-7000-5050
ddos@f5.com




Get F5® Silverline™
DDoS Protection Services



24x7 Security Operations Centre

- Fully automated DDoS attack detection and mitigation in the cloud
- Layer 3-7 protection against all known attack vectors



f5.com/silverline

Key Resources

The F5 DDoS Protection Reference Architecture

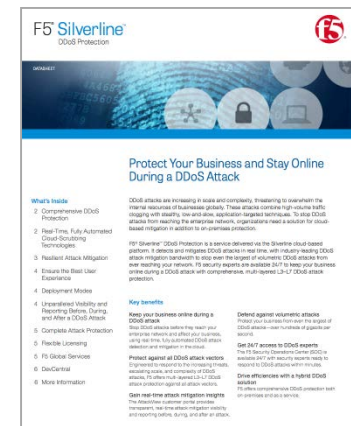
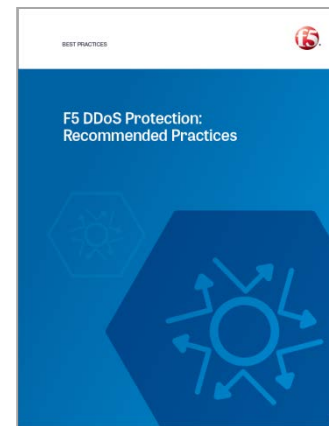
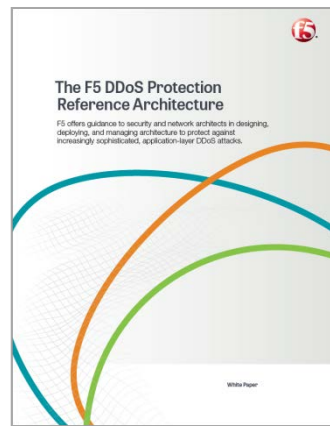
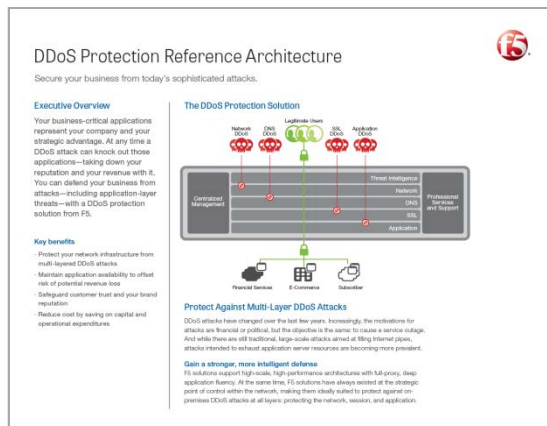
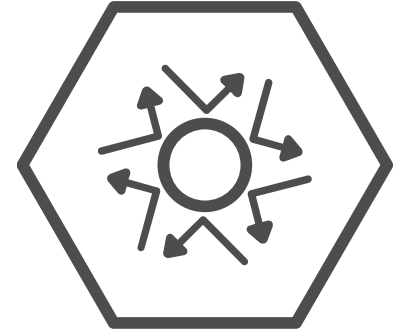
<https://f5.com/solutions/architectures/ddos-protection>

White paper: *The F5 DDoS Protection Reference Architecture*

Best practices: *F5 DDoS Protection – recommended Practices*

The F5 Silverline DDoS Protection Service Overview

<https://f5.com/products/platforms/silverline/f5-silverline-ddos-protection>





Thank You

Q & A



Solutions for an application world.