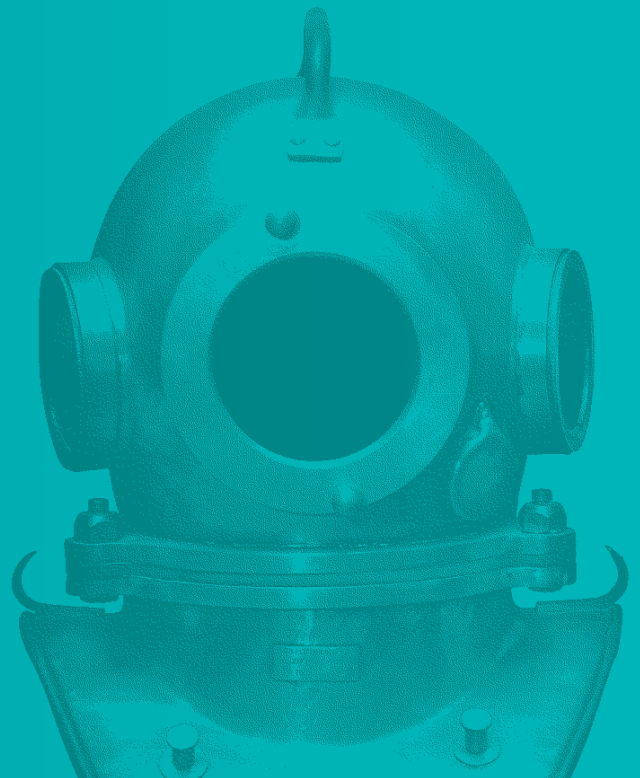
TMOS 13.x

Radovan Gibala, F5 - FSE
Milan Šimčík, Alef - Sr. System Engineer
Jiří Doubek, Alef - Sr. System Engineer



ALEF

Agenda 1. část

- VE enhancements
- Private Cloud
- New BigIP Hardware
- TAP/L2 Transparent Mode, SPAN Port
- Malicious Bots
- Credential Stuffing
- DDoS Attacks
- Malware
- ADFS Proxy support
- Advanced WAF
- New Licensing Model

ALEF

Agenda praktická ukázka

- Advanced WAF
  - Credential stuffing
  - Data safe
- ASM
  - Bot Protection: Web scraping + Bot Whitelisting
  - Brute Force Protection
- Tipy v TMOS v13
  - Troubleshooting monitoru v13, autokorekce časovačů, SSL profil
  - Network map
  - Black list IP v IP add exceptions

ALEF

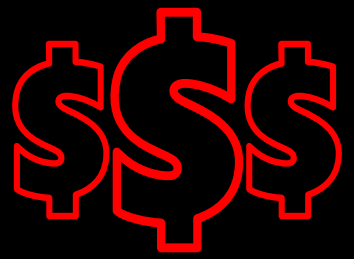
BIG-IP Virtual Edition v13.1/13.1.0.1/13.1.0.2 Key Features Highlights

Cloud Platform Support

- AWS IC* & GovCloud Marketplace offerings
- Google Updates + Utility Licensing
- AzureStack Integration
- VMware on IBM Cloud Integration

High Performance Improvements

- High Performance Native Driver for VMware (non-SRIOV)
- High Performance: Support for 24 vCPUs
- NIC Teaming
- Increased vNIC count



Lower TCO: Licensing & Automation

- BIG-IP Ready Status Indicator
- License Revocation with public license server
- Reduce spin-up time and disk image size
- Update open-vm-tools for automated guest customization

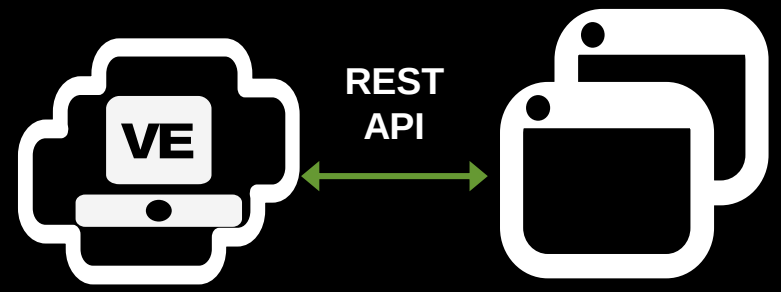
Automation Enablement and Lower TCO

Customer Challenges

- Customers implementing automated deployments must develop tests to check if BIG-IP is ready to accept configurations
- Customers needs to move their VE license key from one host to another during host maintenance or workload migration
- Costs due to frequent spin up/tear down instances and large disk image sizes for developers and iterative DevOps deployments
- Manual VE deployments in VMware environments

F5 Solution: BIG-IP Updates

- BIG-IP Ready Status Indicator - Determine when BIG-IP is able to accept a configuration or ready to license
- License Mobility - Manually or automatically revoke VE license key and apply to different VE without BIG-IQ LM
- Reduce spin-up time by up to 50% and disk image size by up to 40% across various cloud environments
- Updated open-vm-tools enables automated deployment, including mgmt setup w/o DHCP, secure root/admin, and



Reduce Spin Up Time

Result: ~50% reduction in AWS

And Disk Image Size

BIG-IP VE	Upgradeable	Immutable
BETTER, BEST	139G -> 82G	139 -> 60G

Result: ~40% reduction in upgradeable images

VE Performance Improvements

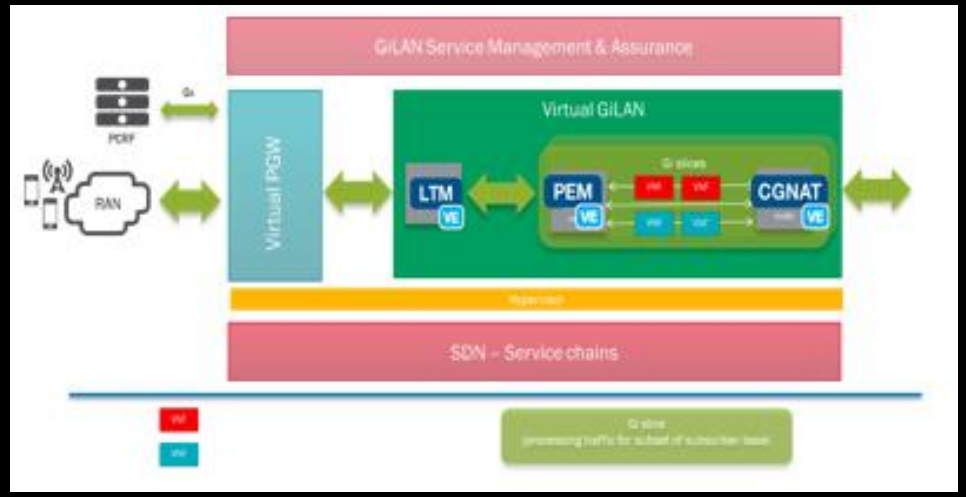
Customer Challenges

- Traffic growth requires high performance VNF's (SP) and software ADC's for high bandwidth application use cases
- CPU cost and inefficiencies using SR-IOV for performance
- Provide ADC services in multiple external networks and Increase bandwidth without requiring upgrade to higher throughput NICs

F5 Solution: Performance Updates

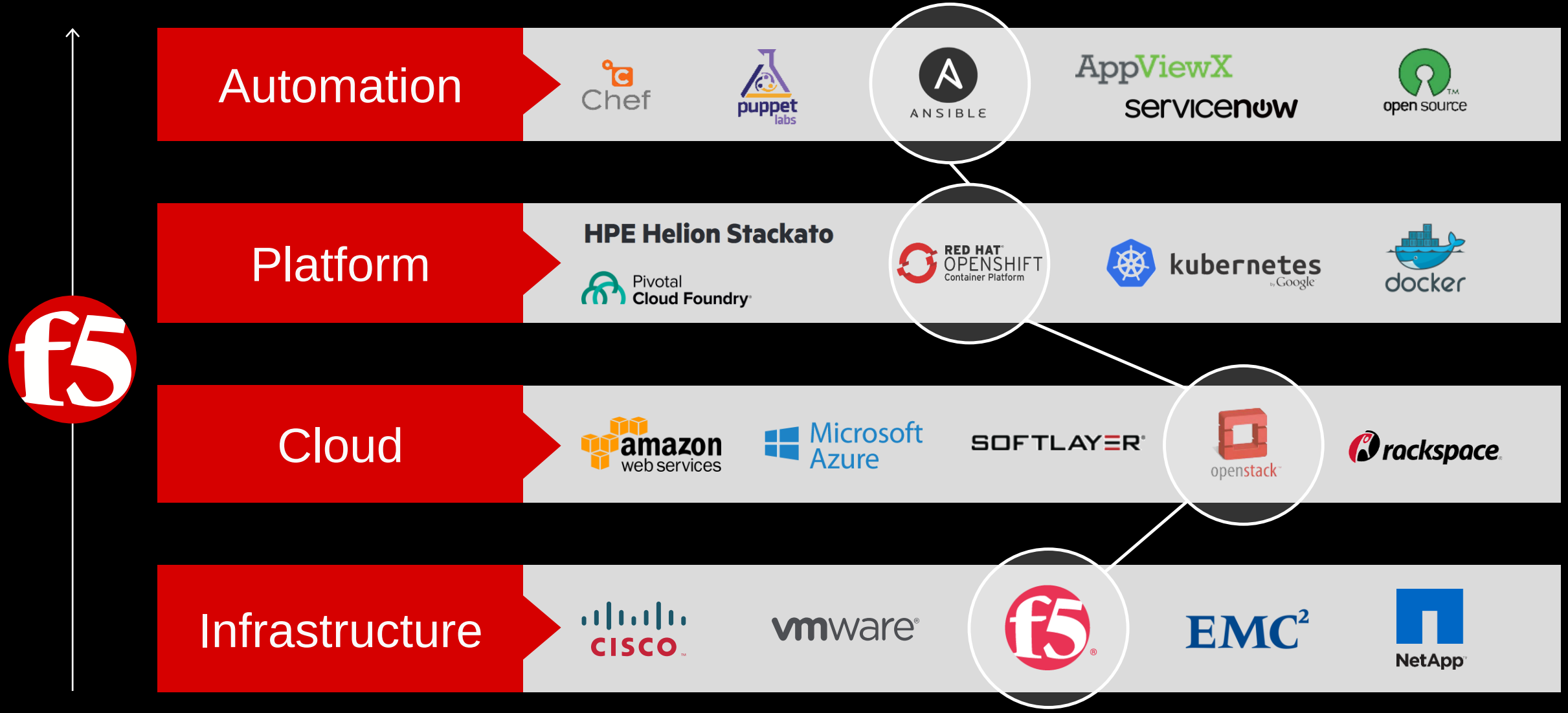
- 20G/10G performance (HP VE/Std VE) without SR-IOV and cpu reduction by supporting native driver for VMware ESXi environments
- High Performance: Support for up to 24 vCPUs (previously 16 was max) for WAF and SSL. Performance improvements TBD.
- NIC Teaming with SR-IOV - Enables customers to team multiple NICs to handle link failures and increase bandwidth without requiring higher throughput NICs & switches
- Increased vNIC interfaces supported to 28 (KVM) - Maintain separate internal/external/mgmt/IPv4/IPv6 networks with one VE

SP: GiLan (LTM, AFM, CGNAT, and PEM)



Enterprise: Traffic Management/App Protection (LTM, AFM, ASM, APM)

It’s All About DevOps and Cloud



New iSeries
BIG-IP i11600/i11800

Sits above i10800 and replaces BIG-IP 10350v

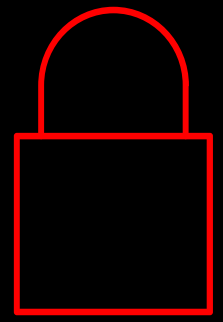
- Compared to i10800
- 2x Processor
- 2x Memory
- 2x SSD capacity
- 2x vCMP instances
- 1.4x L7 RPS and L4 CPS
- Interfaces/Ports same as i10800
- TMOS v12.1.3/13.1

*Available Dec CY17

BIG-IP v13.1 TurboFlex Updates

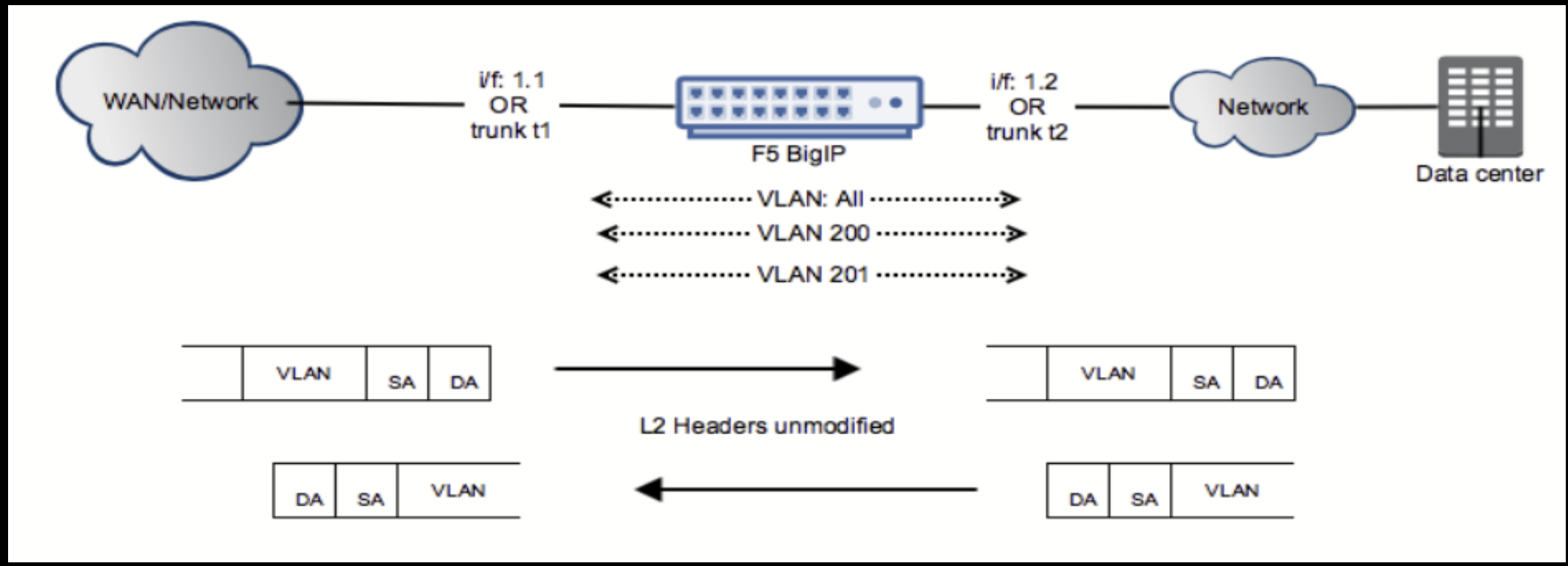
iSeries TurboFlex Enhancement

- GUI for selecting which TurboFlex profile to use
- New features in TurboFlex Security Profile
  - Multiple DoS vector lookups (multi-layer attack mitigation)
  - Custom DoS Signatures In HW (Behavioral DoS) that provides dynamically programmable of HW signatures
  - Transparent L2 forwarding



L2 Wire/L2 Transparent mode

- **L2Wire (aka bump in the wire)**
- In this mode, a port pair is defined, and packets ingressing port-1 of the port pair is sent to port-2 of the port pair and vice versa
- Forwarding decision is based solely on the incoming port.



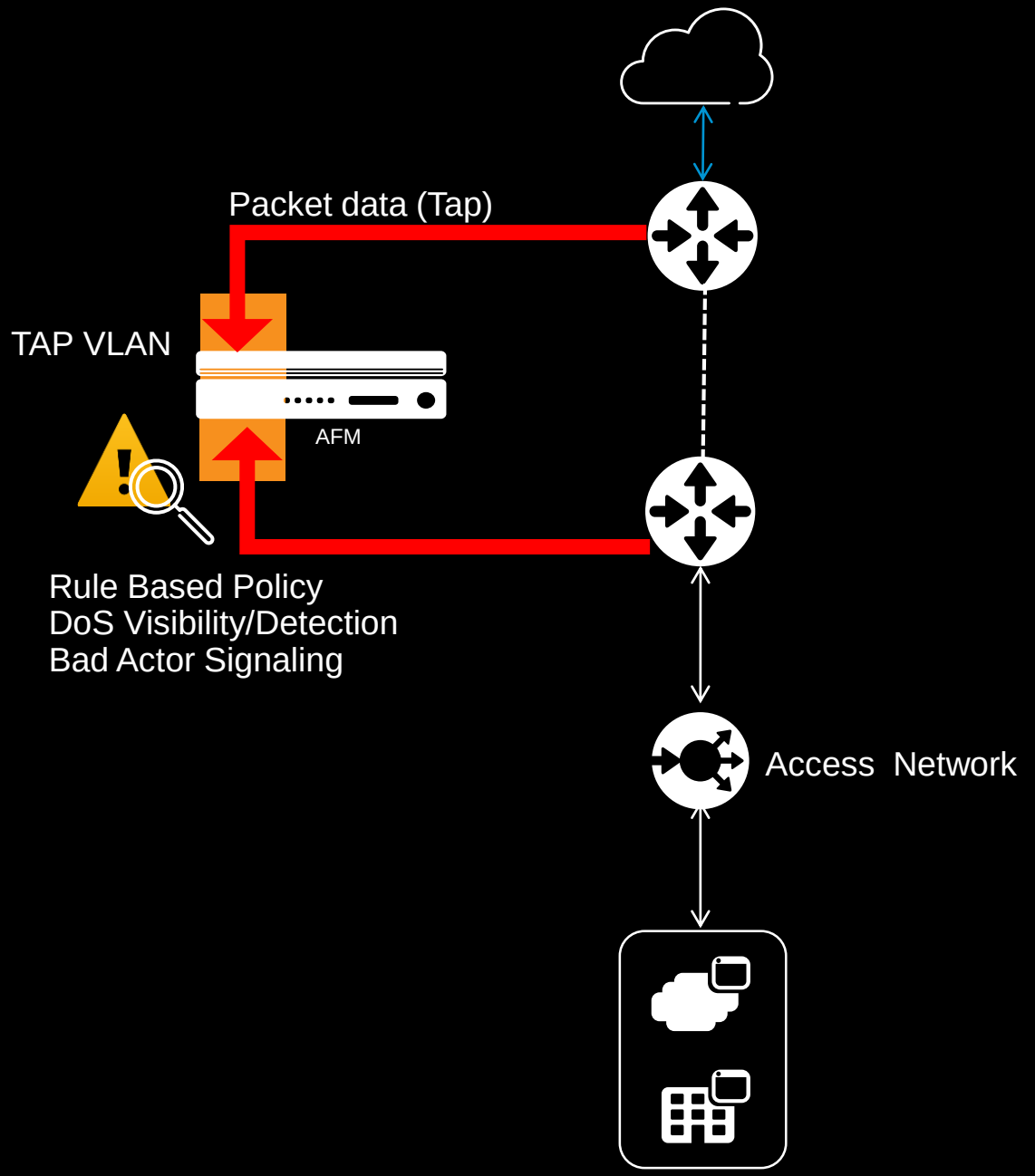
TAP Mode

Customer Challenges

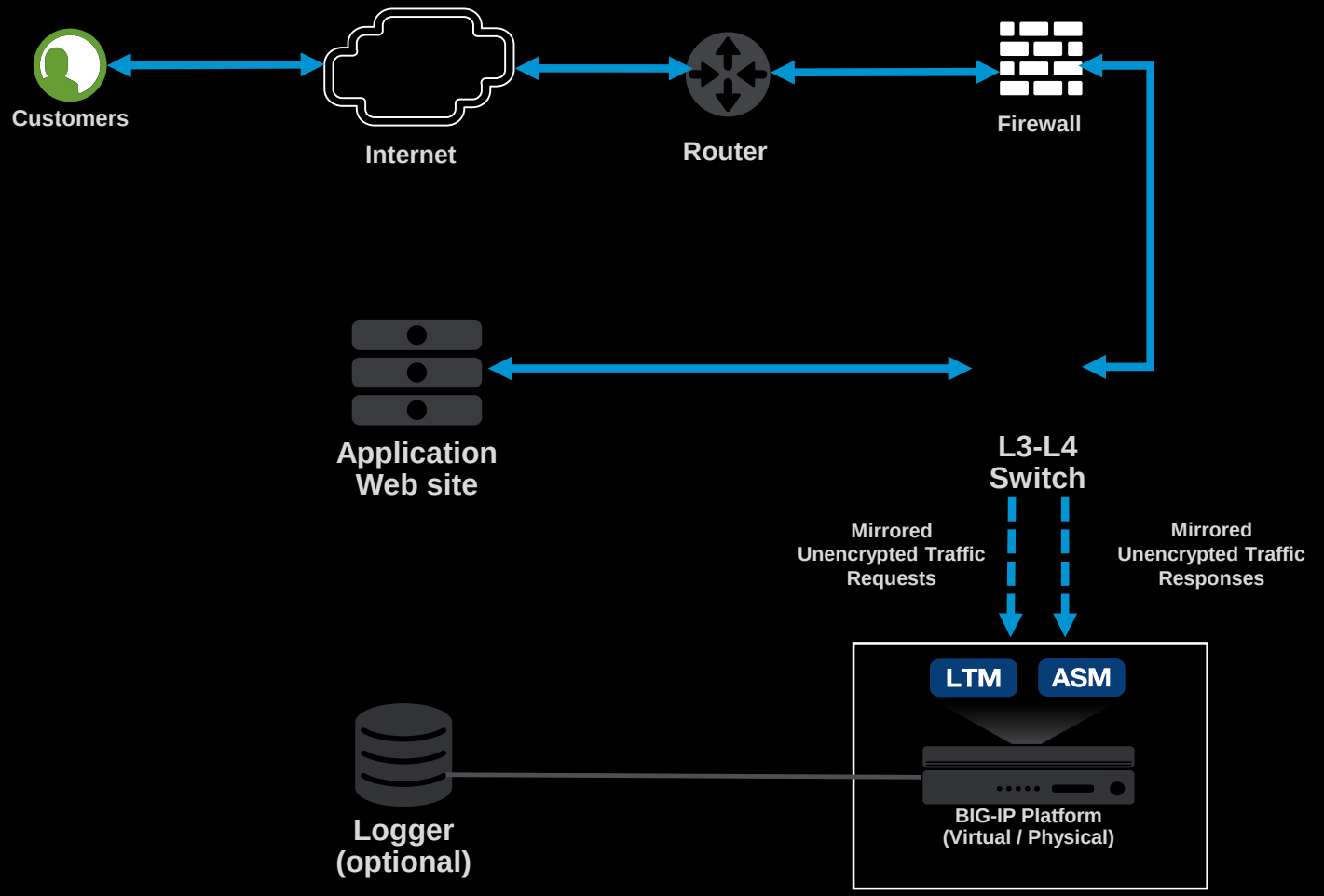
- Avoid single point of failure network scenario
- Identify DDoS attacks from TAP data
- Support topology changes (resistance to inline deployment)

F5 Solution: TAP Mode

- Simplifies deployment
- No single point of failure
- Enhances DDoS detection and visibility
  - RTBH for mitigation via upstream router



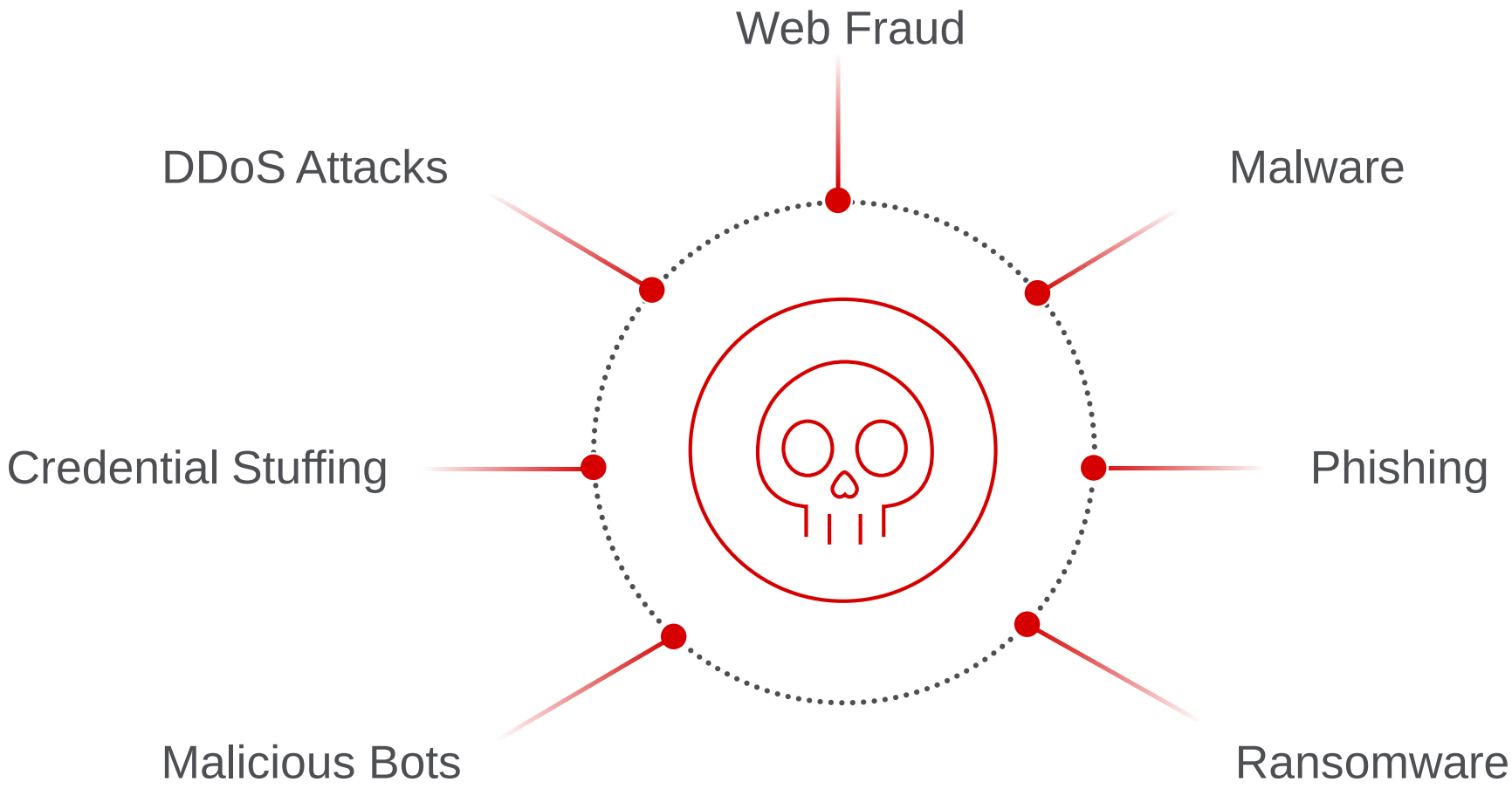
SPAN Port Support (EA) - topology



LTM & ASM configuration includes

- SPAN Port enabled
- FastL4 Profile
- Wildcard Virtual Server (NAT disabled)
- VLAN is optional
- No Pool, No Self IP
- HTTP Profile
- ASM Policy (if needed)
- Application DoS Profile (if needed)

What Are Today's Common Threats?

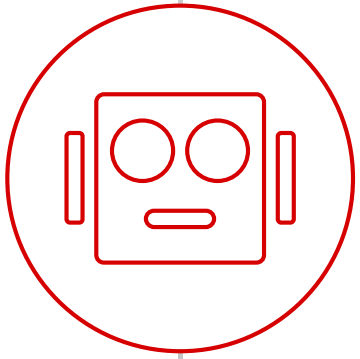


MALICIOUS BOTS

Bots, Bots, and More Bots

50%

of Internet traffic
is automated



77%

of 2016 web application
breaches involved
the use of bots

98.6M bots observed

Source: Internet Security Threat Report, Symantec, April 2017

Bots

A common source of many threat vectors

Client-Side Attacks

- Malware
- Ransomware
- Man-in-the-browser
- Session hijacking
- Cross-site request forgery
- Cross-site scripting

App Infrastructure Attacks

- Man-in-the-middle
- Key disclosure
- Eavesdropping
- DNS cache poisoning
- DNS spoofing
- DNS hijacking
- Protocol abuse
- Dictionary attacks

DDoS Attacks

- SYN, UDP, and HTTP floods
- SSL renegotiation
- DNS amplication
- Heavy URL

Web Application Attacks

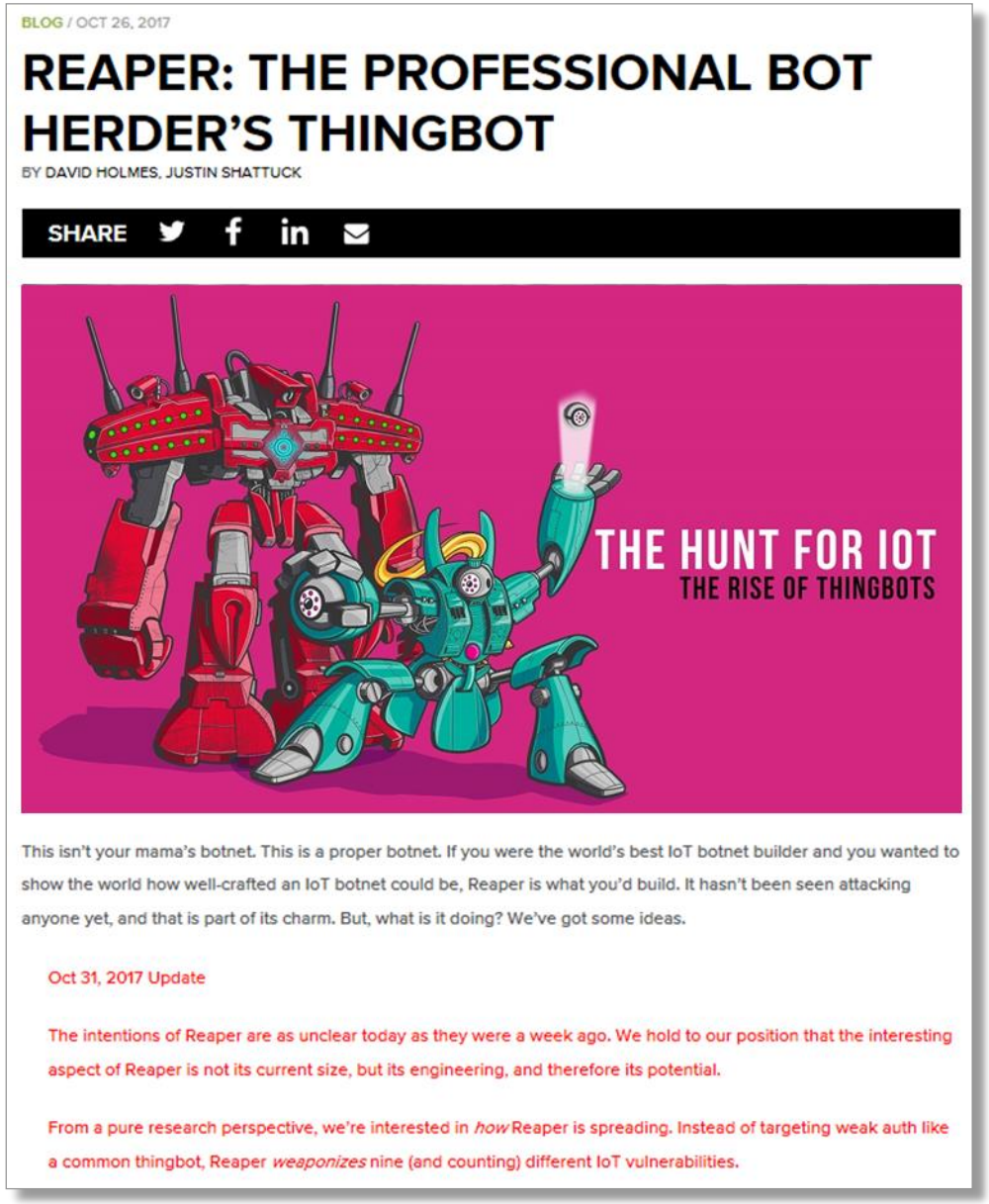
- API attacks
- Cross-site scripting
- Injection
- Cross-site request forgery
- Malware
- Abuse of functionality
- Man-in-the-middle
- Credential theft
- Credential stuffing
- Phishing
- Certificate spoofing
- Protocol abuse

Thingbots

Application Threat Intelligence

Reaper panic

The latest thingbot making press waves was predicted in "The Hunt for IoT" volume 3



Proactive Bot Defense

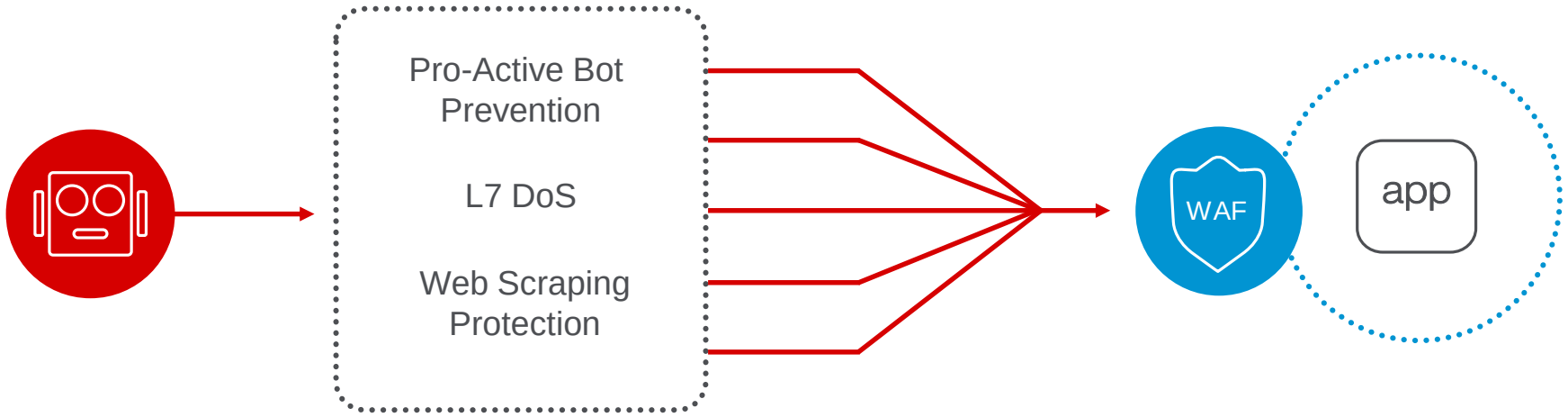
PROBLEM

Malicious bots

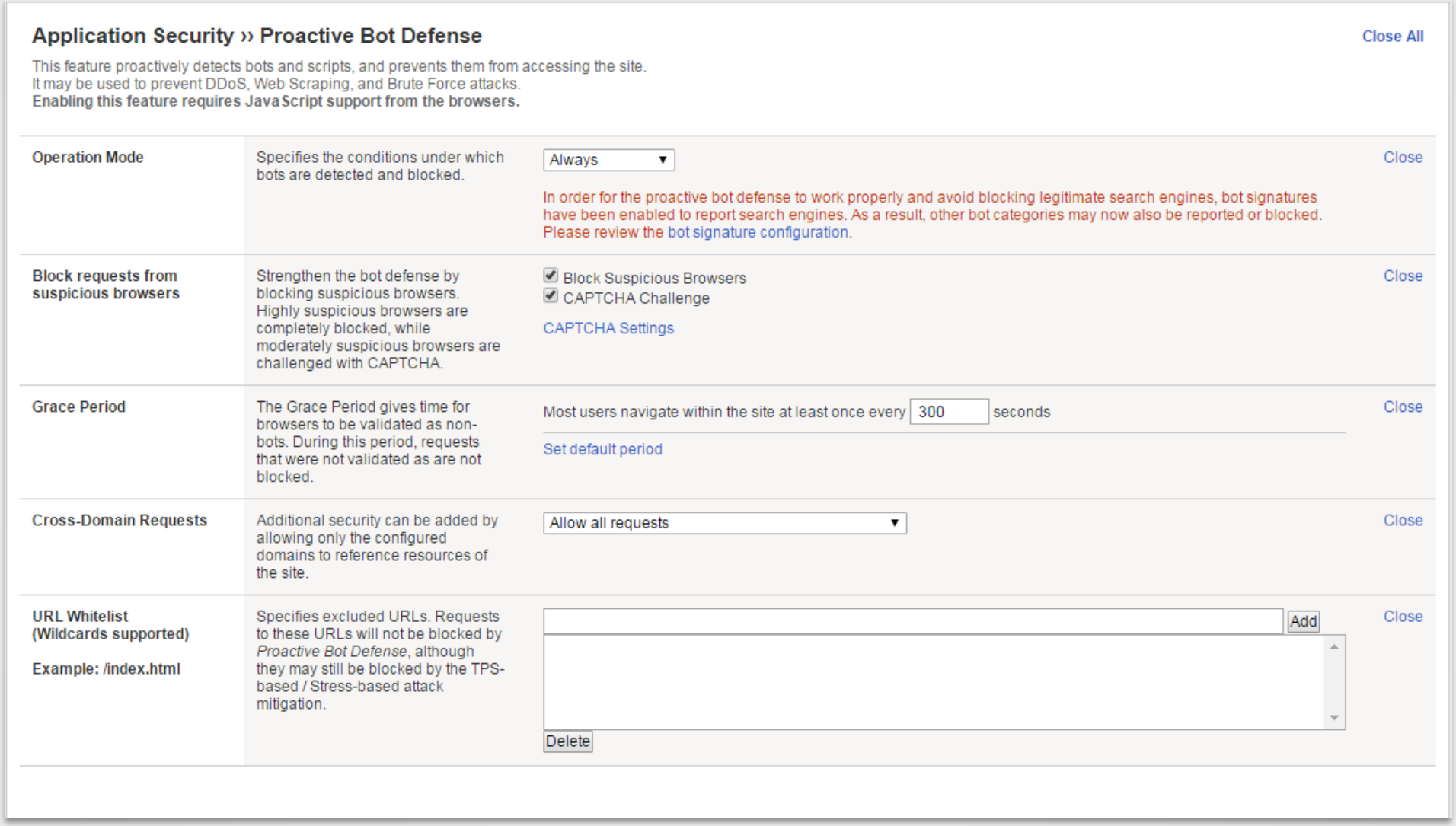
SOLUTION

Web Application Firewall (WAF)

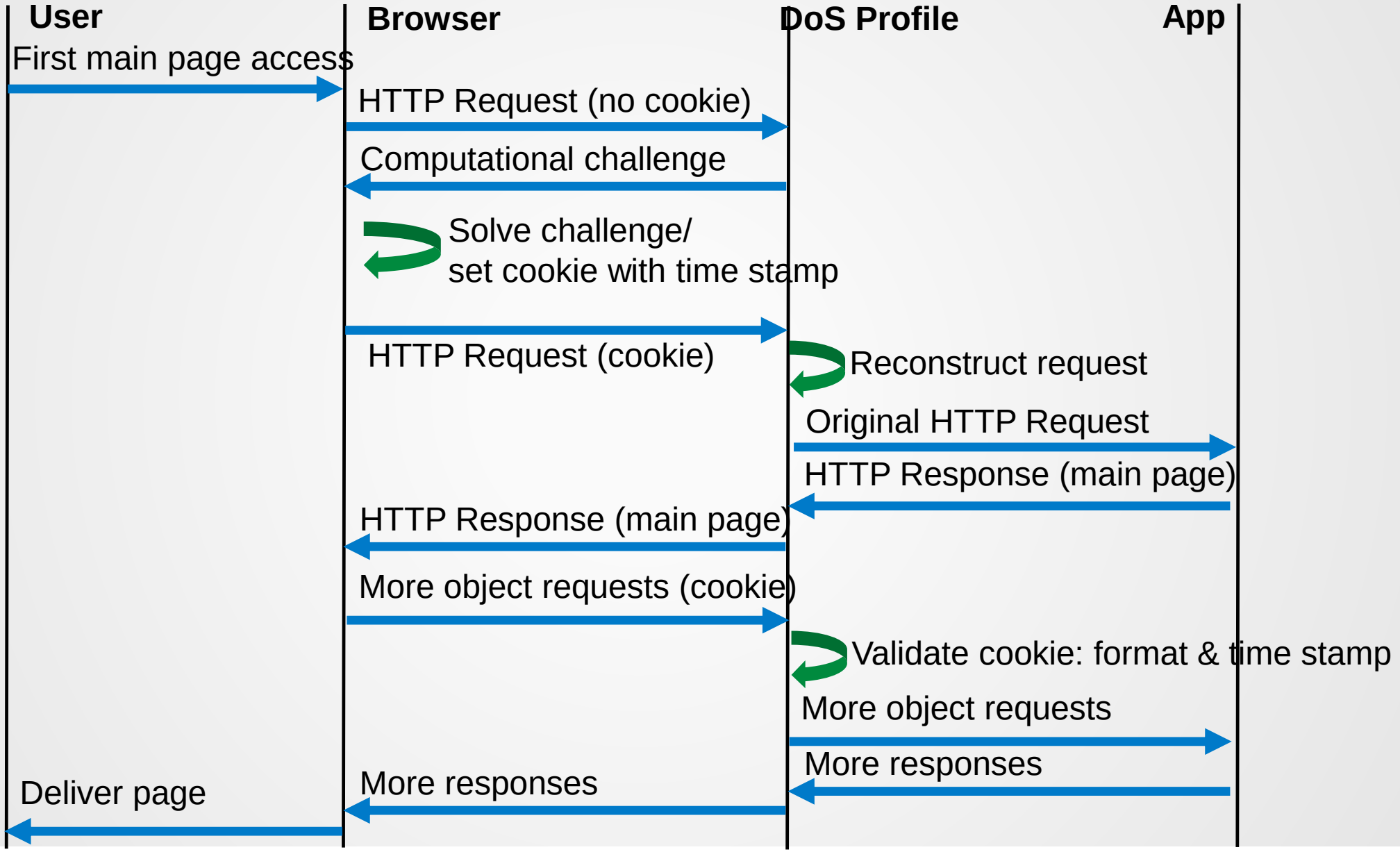
Behavioural analysis to identify malicious bots



Proactive Bot Defense and Bot Signature

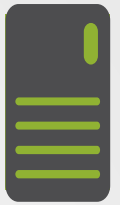


PBD - Client side integrity defense - flow



Bots that simulate browsers

I’m a Bot that simulate browser



DNS Server

Web Server

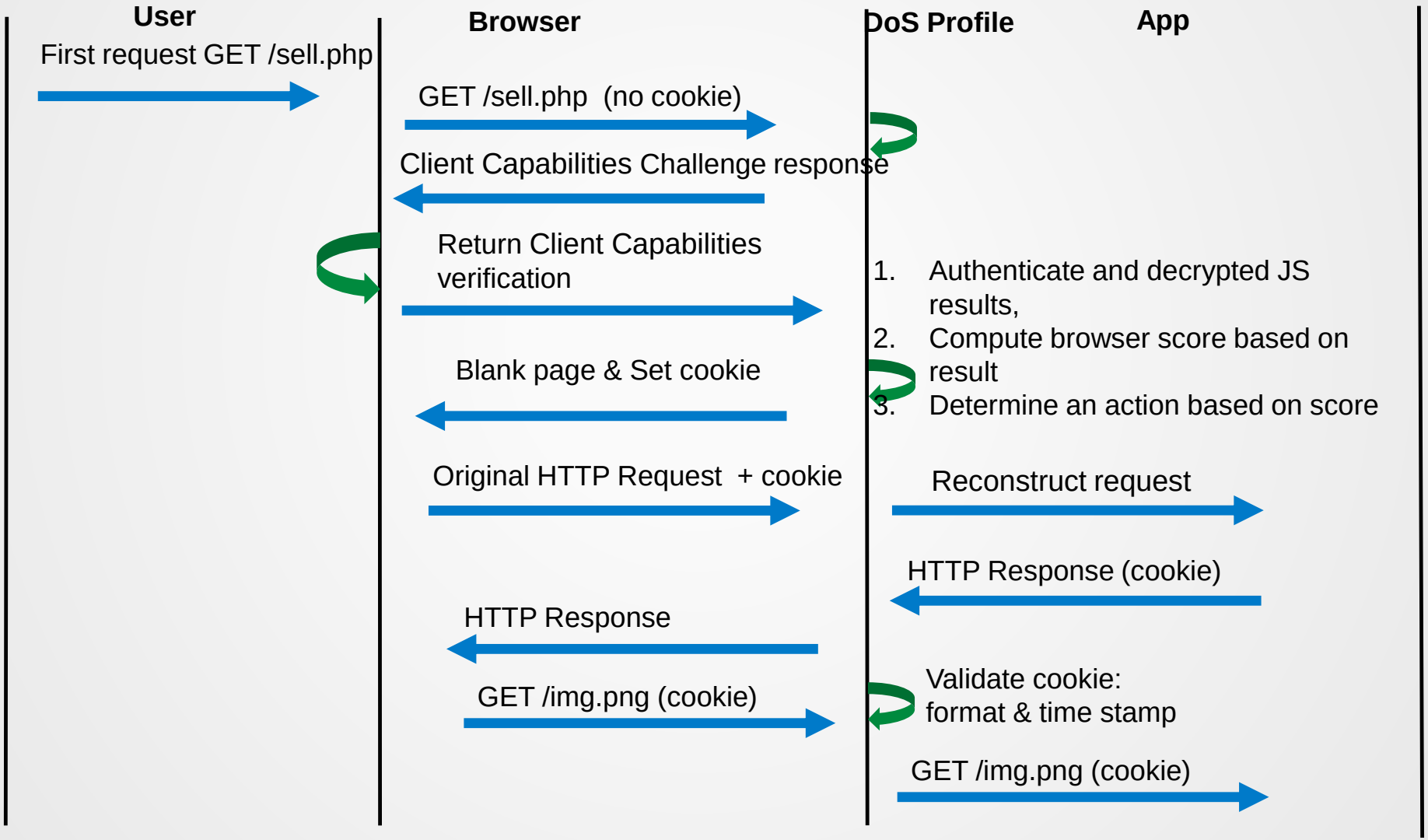
Capability ?
CATPCHA ?

ASM: ok, what are your capability ? If you will not answer right you will have to answer a CAPTCHA

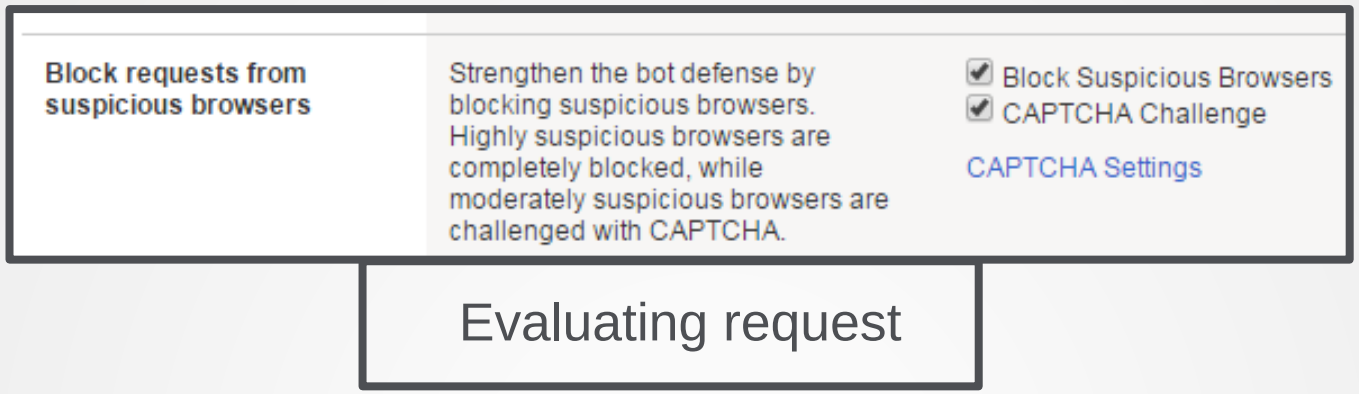
Bummer

No you are not, bye bye -> block this guy.

Client Capabilities -challenge script flow



How bots that simulate browsers are evaluated and scored



High Score

Pass

0 – 59 – browser

60 – 99 – Unknown

100 – Bot

Low Score

Send CAPTCHA and

If valid CAPTCHA – Pass

Otherwise - Block

Proactive Bot Defense improvements summary

- PBD interaction with Bot signature – Benign white list

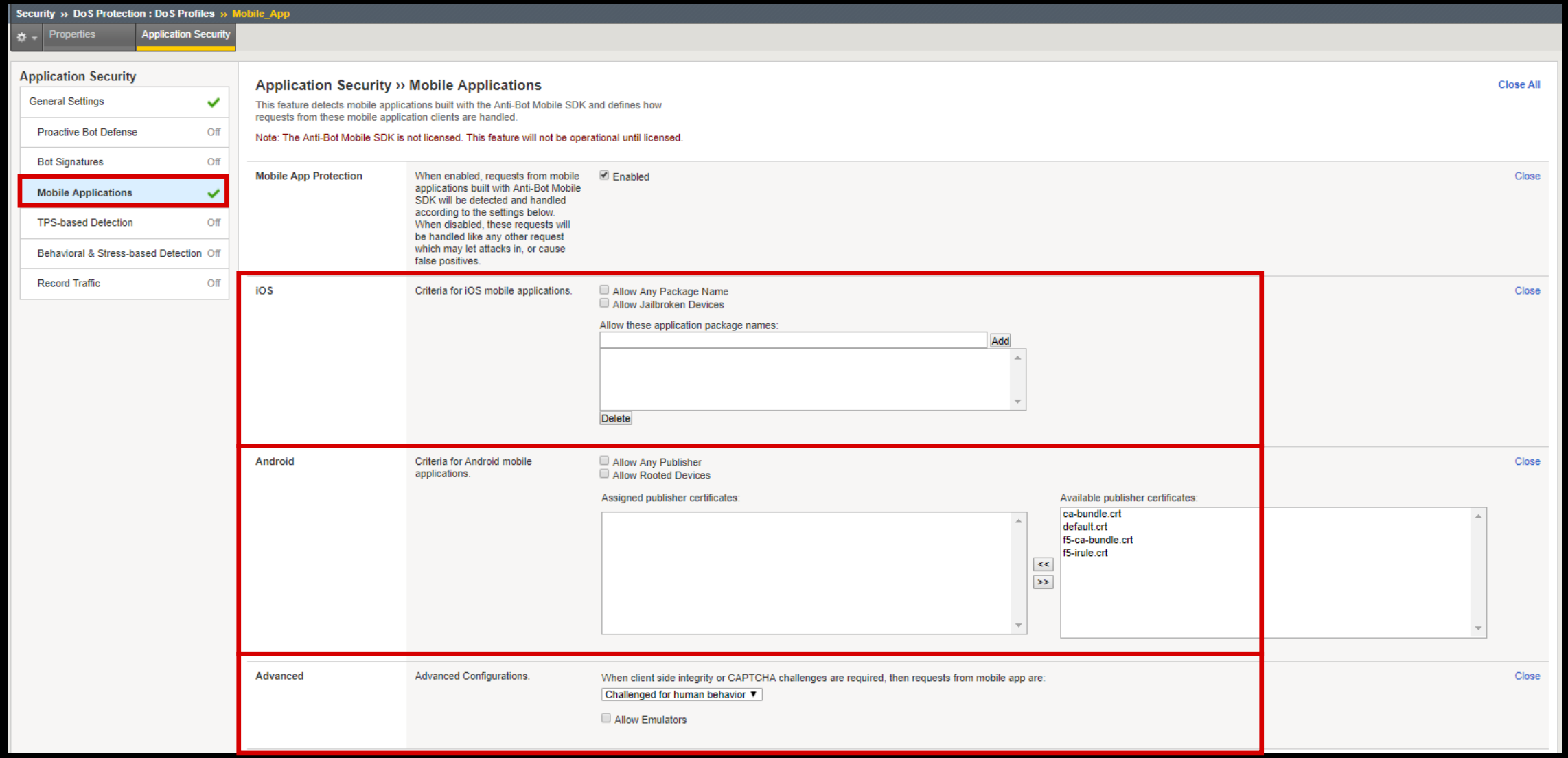
- Identification of browsers discrepancies utilizing **I can use** and **Modernizr** databases (updates same time as other attack signatures)
- Databases are updated with the ASM attack signatures and the bot signatures
- Giving score to browsers and executing relevant actions:
  - Pass request to the server
  - CAPTCHA to verify human
  - Block bots

Anti-Bot Mobile SDK

Mobile SDK is part of a unified framework for detecting bots and classifying clients

- Requires a separate license
- Requires a separate Anti-Bot Mobile SDK EULA
- SDK will be available upon request
- SDK should be integrated by application developer with the existing mobile application

Anti-Bot Mobile SDK



CREDENTIAL STUFFING

Credential Stuffing Example

- No prior breach
- Dozens of account takeovers left users picking up food bills they never ordered
- Unsuspecting victims received receipts via email, after it was too late

Fraudsters eat for free as Deliveroo accounts hit by mystery breach

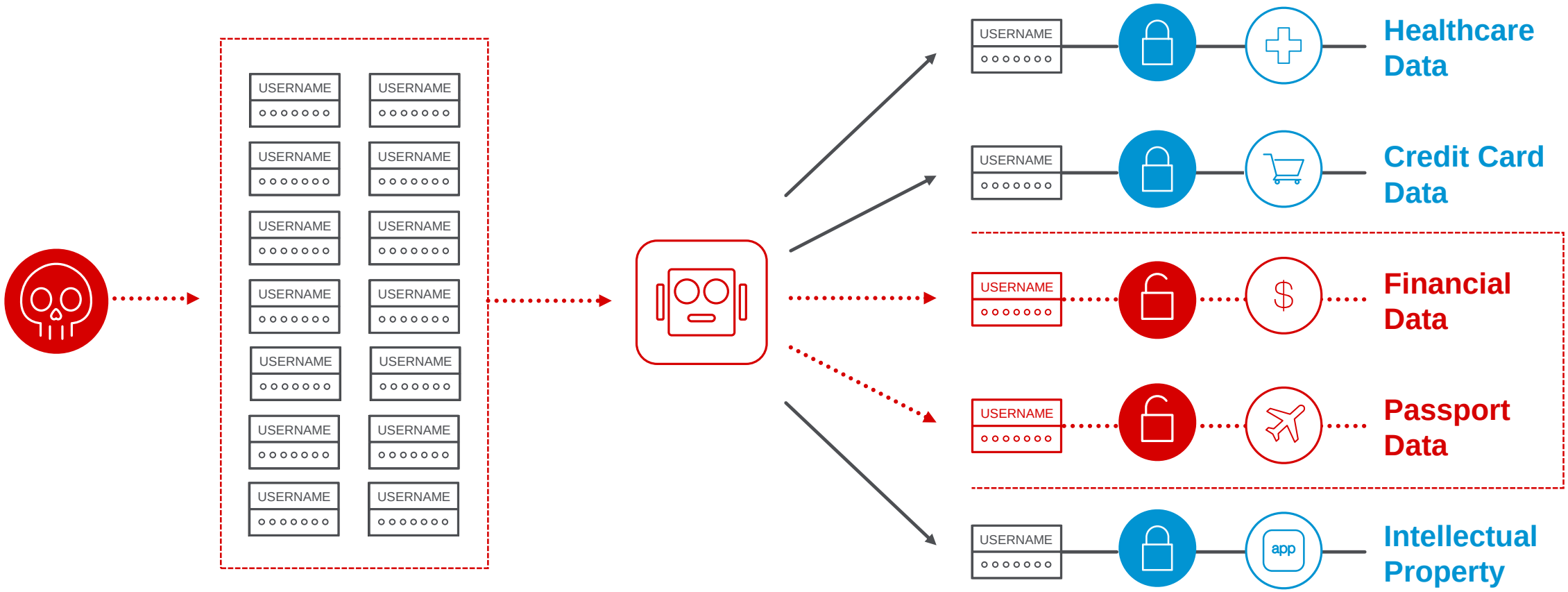
Major Credential Breaches

In the last 8 years more than 7.1 billion identities have been exposed in data breaches[1]

"Nearly 3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more"[2]

1) Symantec Internet Security Threat Report, April 2017
2) Password Statistics: The Bad, the Worse and the Ugly, Entrepreneur Media

How Credential Stuffing Works



Mitigation Options

Application Threat Intelligence

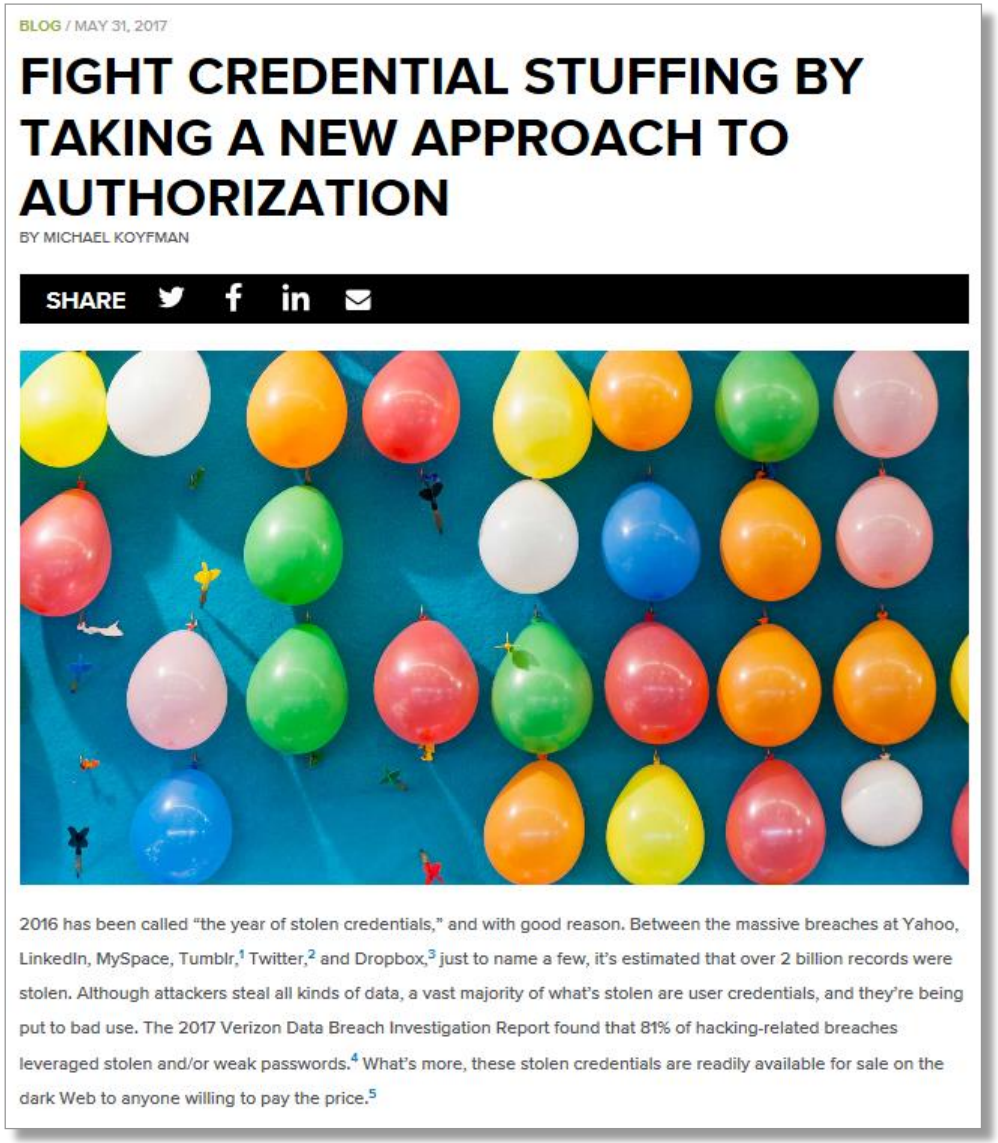
F5 LABS

Info on emerging threats

What is it?

Who does it affect?

Protection strategy recommendations



BLOG / MAY 31, 2017

FIGHT CREDENTIAL STUFFING BY TAKING A NEW APPROACH TO AUTHORIZATION

BY MICHAEL KOYFMAN

SHARE

2016 has been called "the year of stolen credentials," and with good reason. Between the massive breaches at Yahoo, LinkedIn, MySpace, Tumblr,[1] Twitter,[2] and Dropbox,[3] just to name a few, it's estimated that over 2 billion records were stolen. Although attackers steal all kinds of data, a vast majority of what's stolen are user credentials, and they're being put to bad use. The 2017 Verizon Data Breach Investigation Report found that 81% of hacking-related breaches leveraged stolen and/or weak passwords.[4] What's more, these stolen credentials are readily available for sale on the dark Web to anyone willing to pay the price.[5]

Credential Stuffing Mitigation

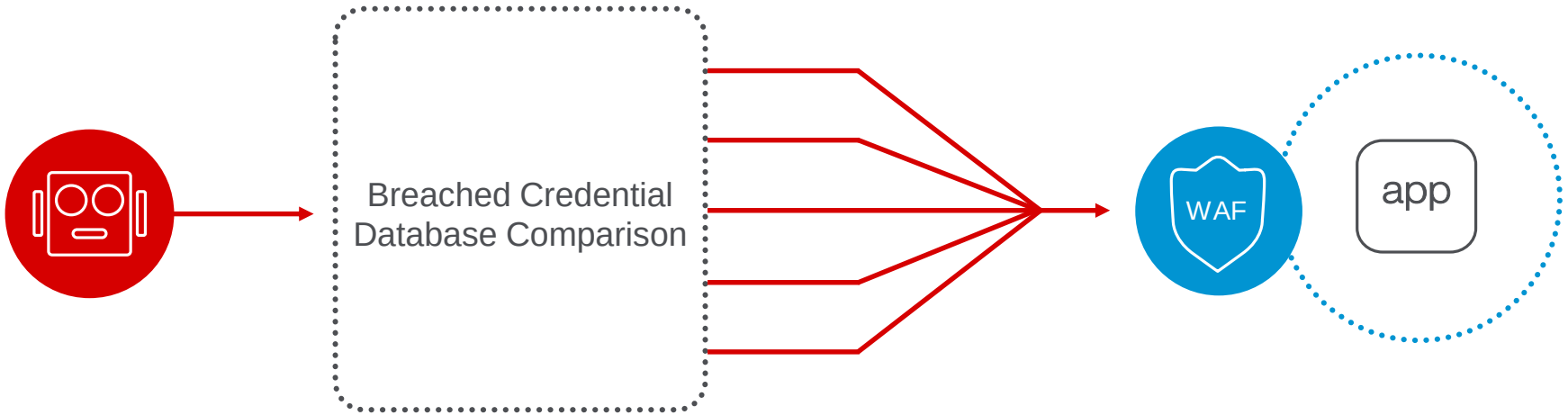
PROBLEM

Credential stuffing

SOLUTION

Web Application Firewall (WAF)

Distributed brute force protection



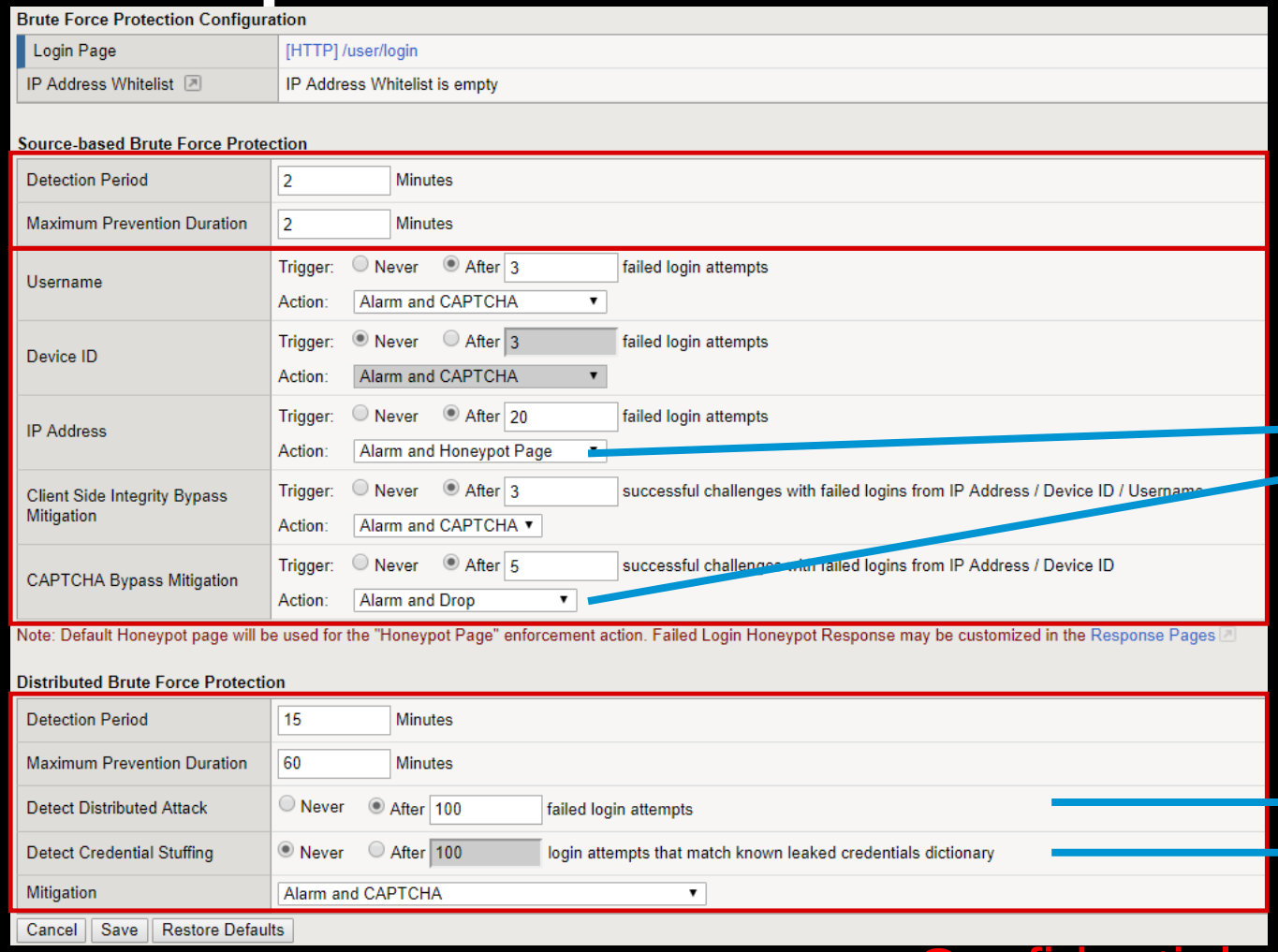
Brute Force Protection Rearchitecture

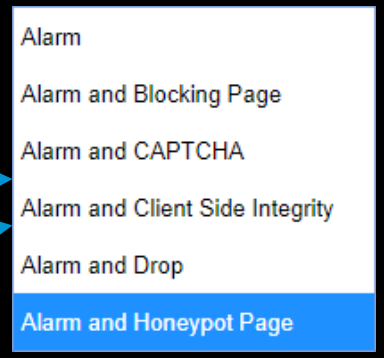
- **Attack Detection**
- Single source
- CAPTCHA bypass (CAPTCHA farm detection)*
- Distributed attack
- Credential Stuffing *(EA)*
- Learning of Brute Force violation is deprecated
- **Mitigation**
- Enforcement actions: Alarm, CSI, CAPTCHA, Blocking page, Honeypot page, Drop
- Guarantee login availability to legitimate users
- Escalate mitigation upon detection of CAPTCHA bypass
- CAPTCHA for distributed attack

New in ASM 13.1

Brute Force Protection Rearchitecture

- A simpler GUI that works from default settings



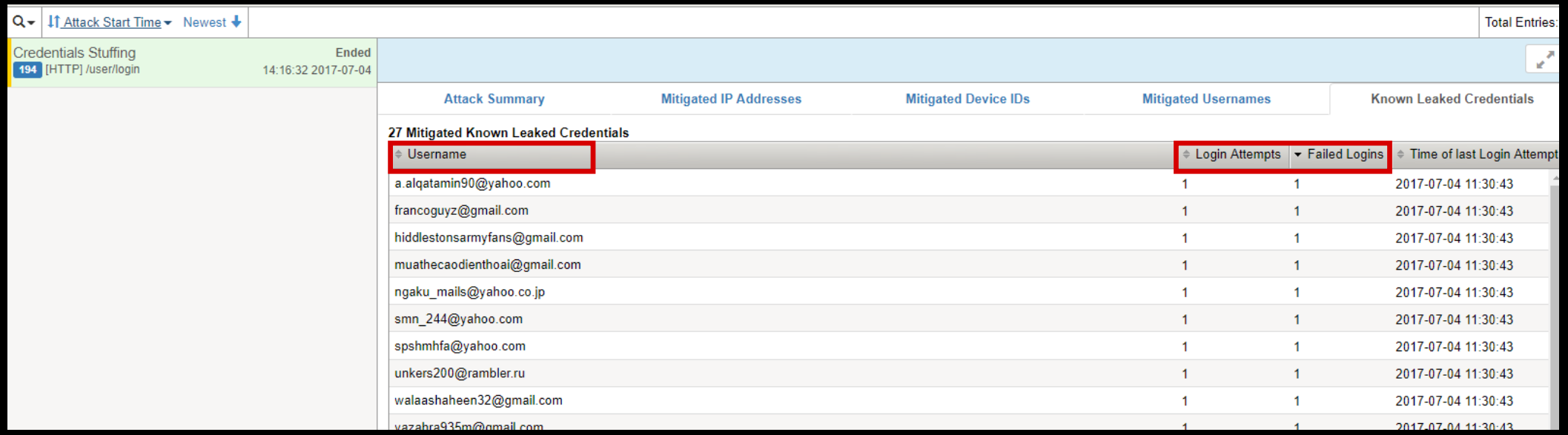


New Mitigation techniques and actions

Distributed Attack and Credential Stuffing detection

Brute Force Protection Rearchitecture

- **Credential Stuffing**



- When an attempt at brute force is detected, credential stuffing suspicious attempts are checked and compared to a known database.

Mitigating with Authorisation

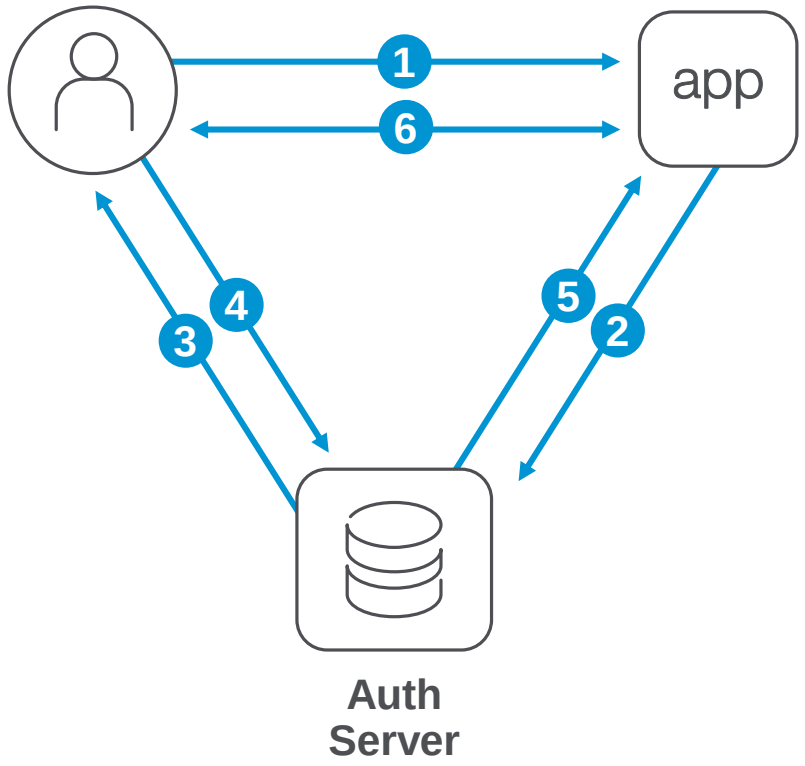
PROBLEM

Credential stuffing

SOLUTION

Access control

Token-based authorisation (OAuth)



1. User login to application
2. User redirected to authorisation server
3. Authorisation server requires authentication before authorisation
4. User logs in
5. Auth server grants token
6. User access application

OAuth 2.0 Support

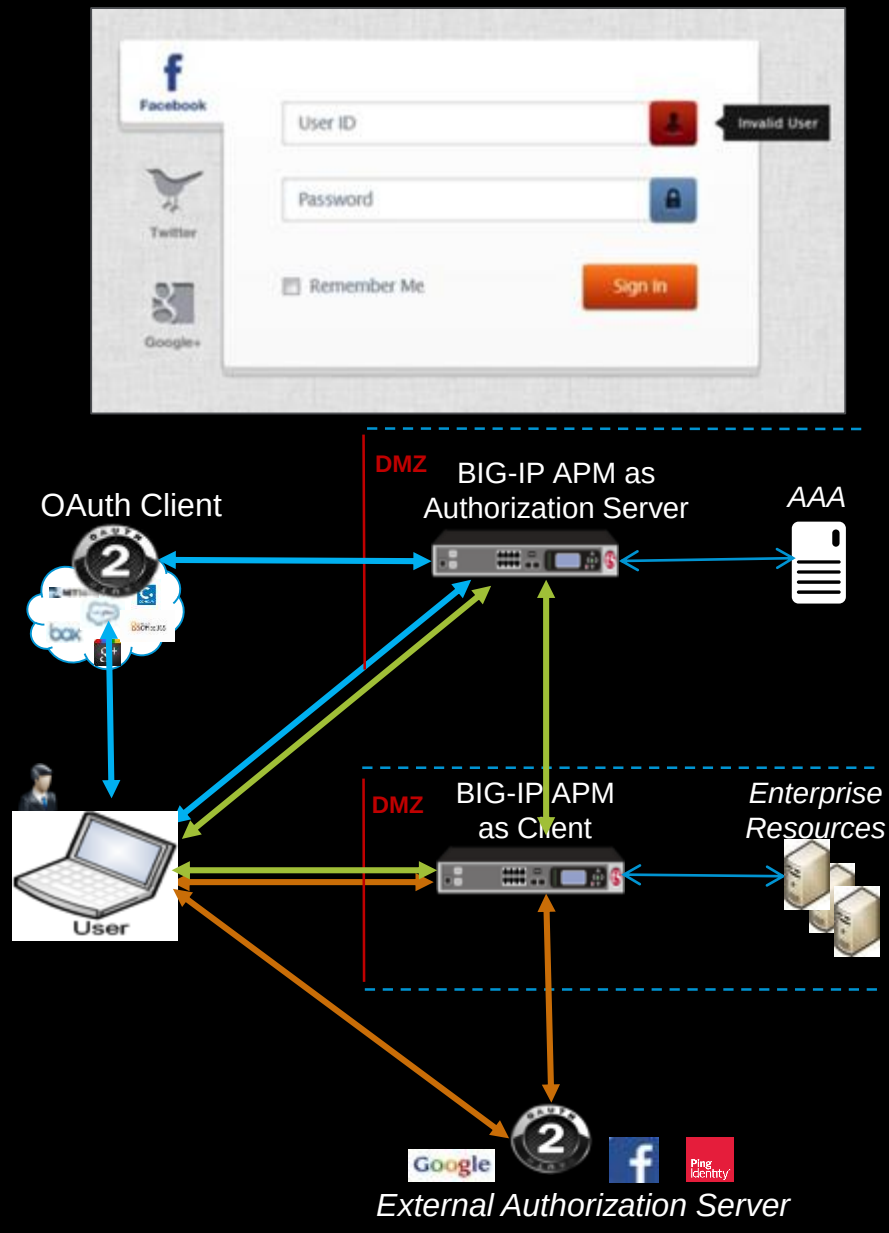
Social login use, SaaS authorization, and API protection

Customer Challenges

- Improve user experience and registration workflow when logging into new sites
- Ability for users to share community content
- Improve application API sharing protection
- Simplify user access to SaaS apps that support OAuth

F5 Solution: OAuth 2.0 Support

- APM serves as OAuth client for social login
- APM is an authorization delegate for SaaS apps
- APM protects and authorizes web services APIs



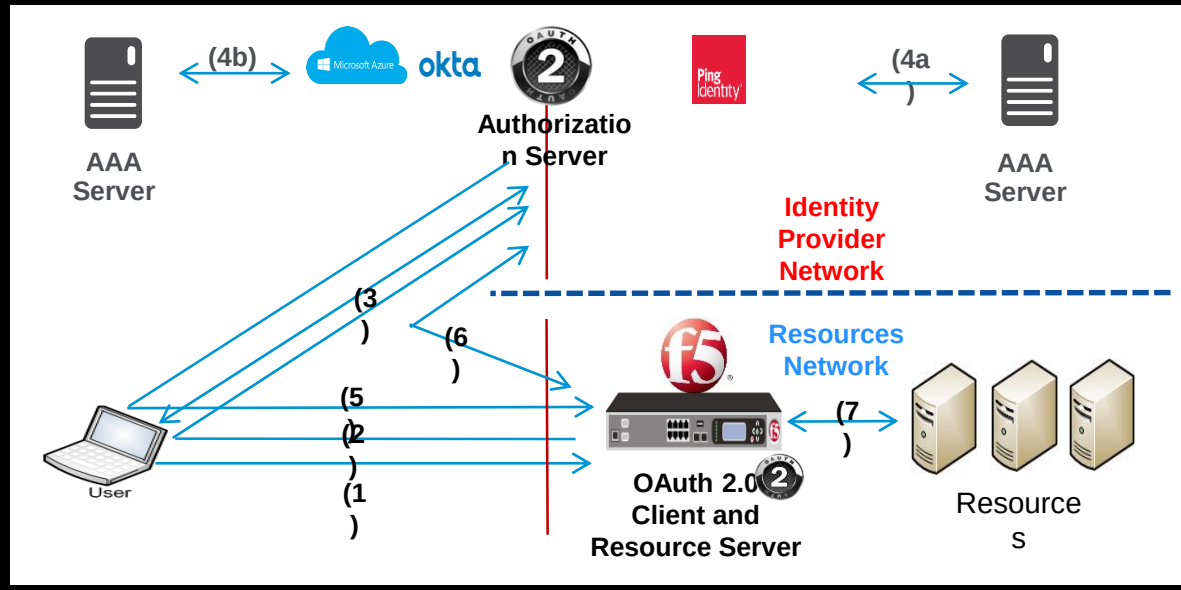
OpenID Connect (OIDC) Support for OAuth Resource Server + Client

Customer Challenge

- Centralization of authorization & SSO across apps including with non-OIDC enabled apps
- Move to industry and App Developer friendly standardization for AuthN/Z across apps
- App authorization or customization based on user identity from another Identity Provider

APM Solution

- OpenID Connect for Client / Resource Server
- Built-in support for Identity Providers: Azure AD, Google, and Ping
- OpenID Connect for Authorization Server coming in BIG-IP v14.0 (Flatrock) Release



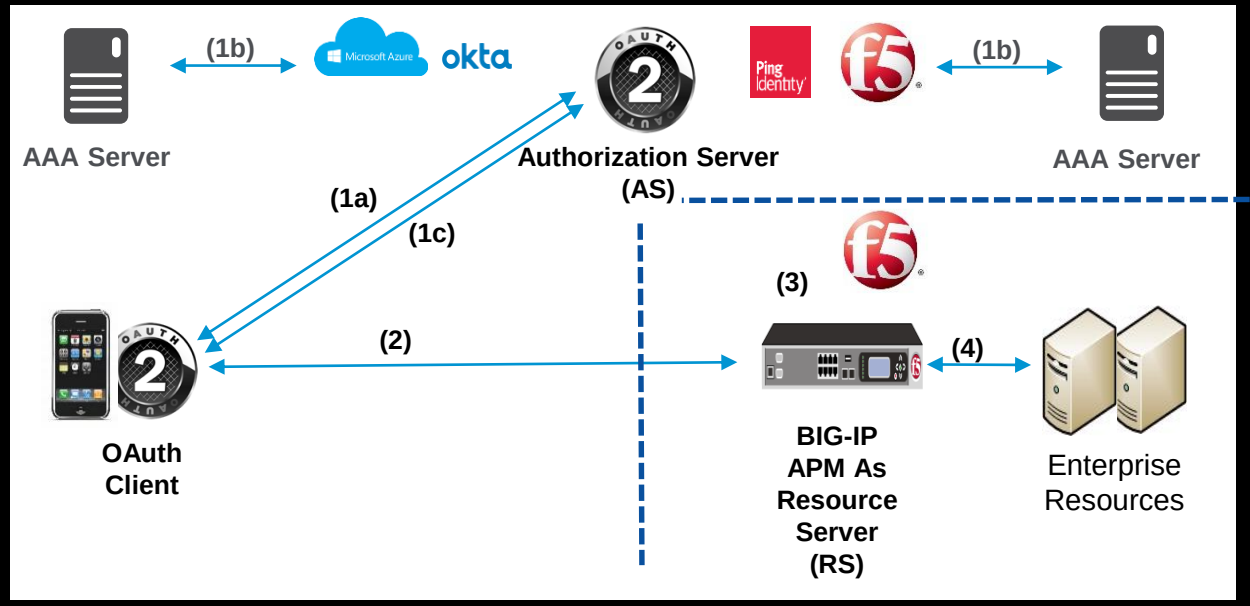
JSON Web Token (JWT) Support With OAuth

Customer Challenge

- Mobile apps access or APIs access without an always-on or connection to the Identity Provider
- Scaling for high volume API calls or clients
- JWT required with for popular OAuth Identity Providers (i.e. Azure AD)

APM Solution

- JWT tokens for APM as OAuth Authorization or Server Client / Resource Server – use digital signatures instead of statefull tokens that need validation
  - Access and Refresh Tokens (RFC 7519)
  - JWK (RFC 7517) and Well-known end points
  - Support for signing JWS (RFC 7515)
  - Support for asymmetric key rotation
- Built-in JWT support for Identity Providers: Azure AD, ADFS, Amazon, F5, FB, Google



Enhanced Step-up Authentication

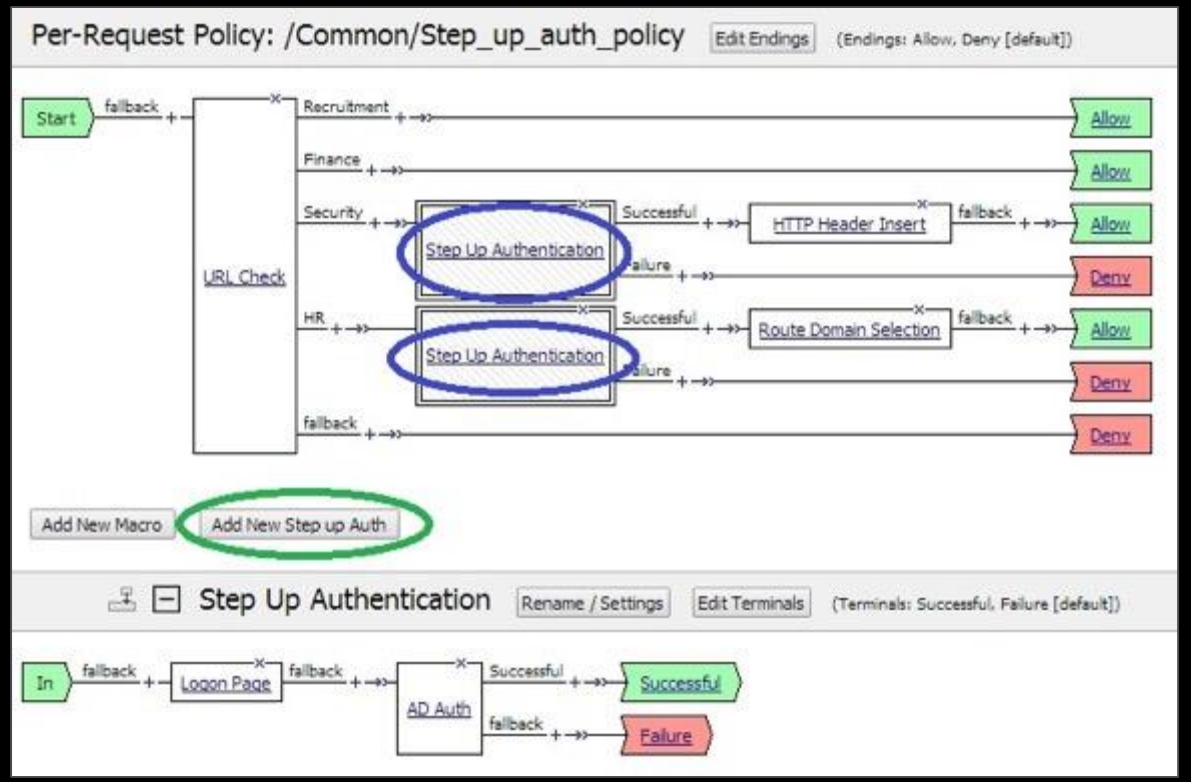
Strengthens user authentication protection for AD authentication

Customer Challenges

- Multi-level applications carry higher risk
- Desire to add additional or multi-factor authentication (MFA) to secure parts of apps
- Need to re-validate user credentials for certain high security sections of apps

F5 Solution: Step-up Authentication

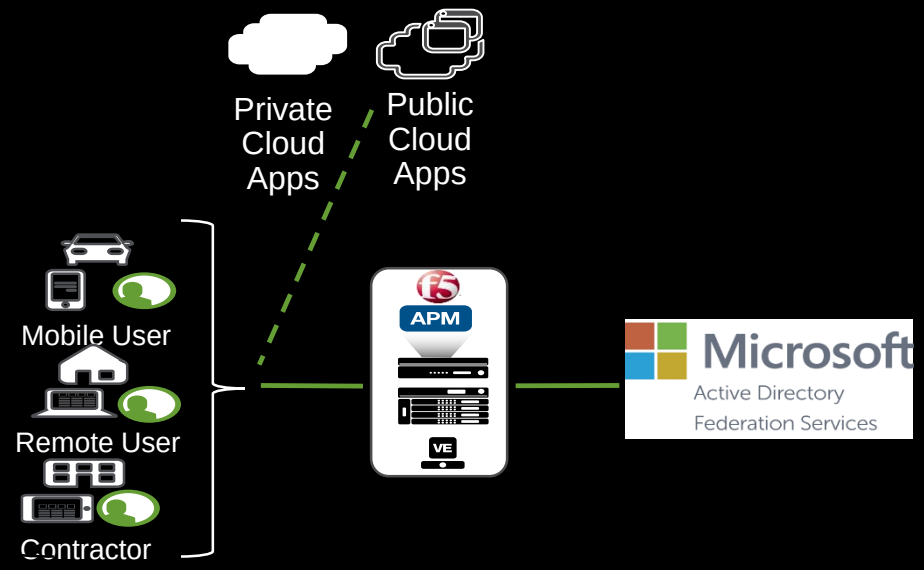
- Protects sections of apps with client certificates with validation, MFA providers that use HTTP or RADIUS AAA (DUO, Yubico, RSA SecurID), or local database
- Credentials can be checked based on any session variable



ADFS Proxy Integration Protocol (PIP) Support

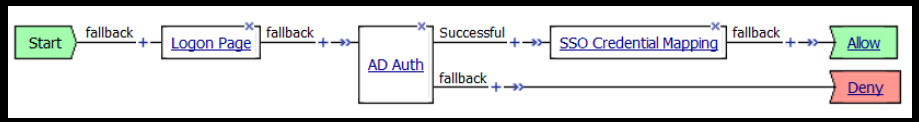
Customer & Sales Challenge

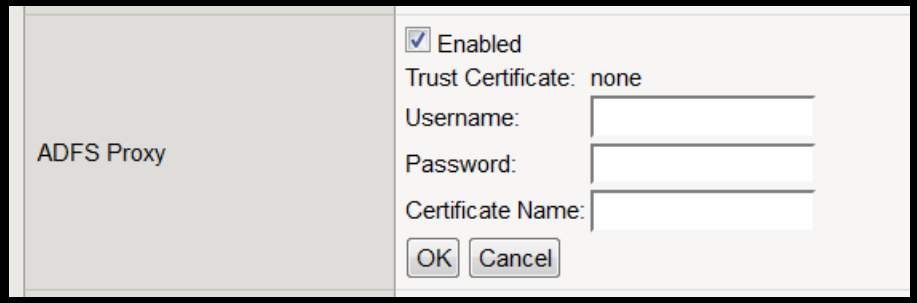
- Scaling of on-prem MS ADFS for O365, MS on-prem apps, and other apps for federation without large TCO
- Device posture checks and use of existing MFA vendor investments
- Security concerns with having Windows in DMZ (MS WAP)
- Issues with getting MS support previously with APM as ADFS proxy



APM Solution

- Proxy for Active Directory Federation Services 3.0 & 4.0
- Replaces the Proxy functionality in Microsoft WAP
- Secure access to Office365 from on-premises ADFS
- Meets Proxy Integration Protocol (PIP) specifications
- F5 APM provides proxy capability for pre-authentication (endpoint inspection and MFA support) enabling scaling of MS ADFS
- First PIP implementation outside Microsoft





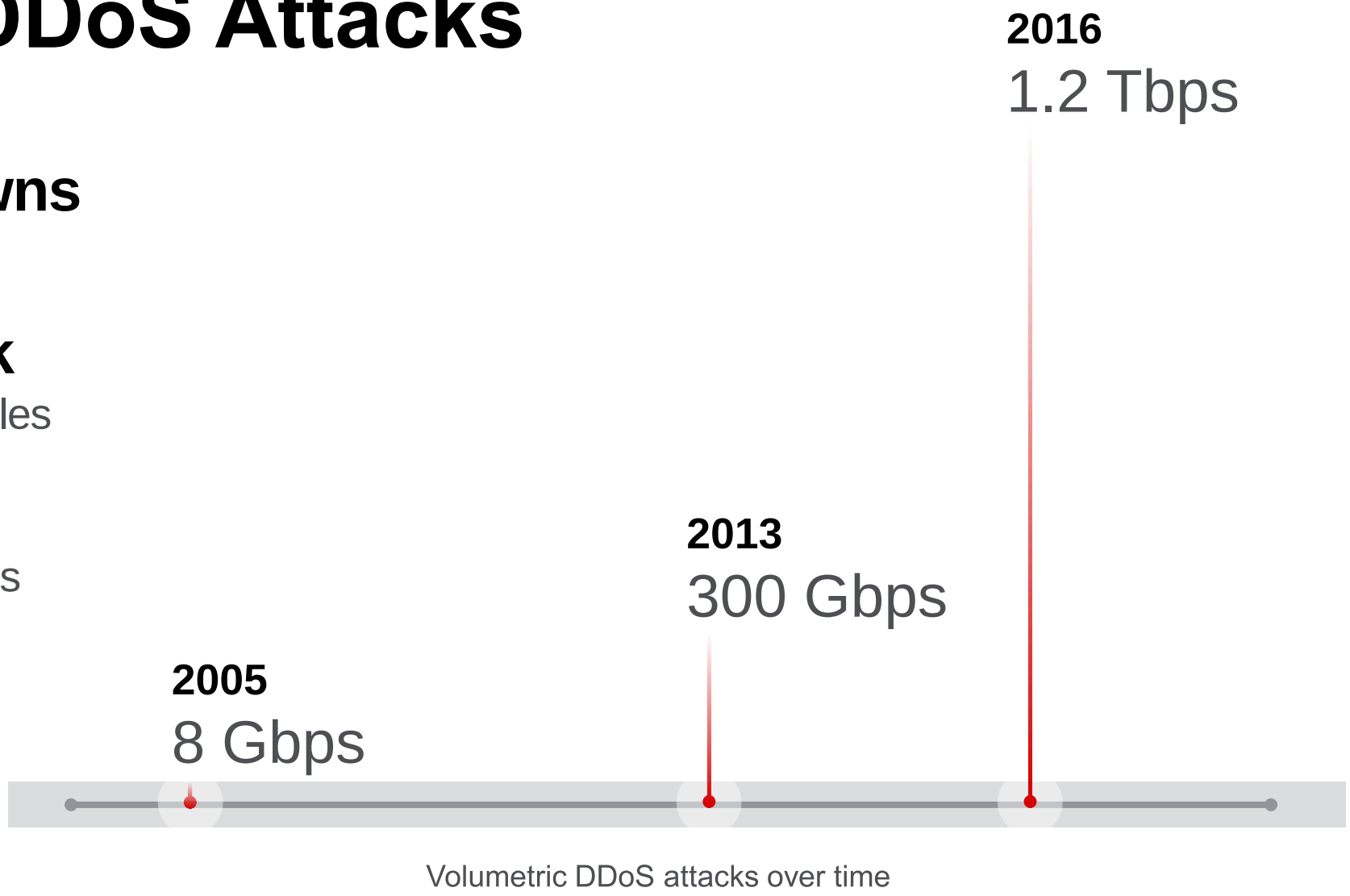
DDOS ATTACKS

Evolution of DDoS Attacks

Volumetric take-downs
Consume bandwidth of target

Network layer attack
Consume connection state tables

Application layer
Consume application resources



Volumetric DDoS attacks over time

Source: How DDoS attacks evolved in the past 20 years, BetaNews

DDoS in the News

Mirai DDoS attacks

620 Gbps

1 Tbps

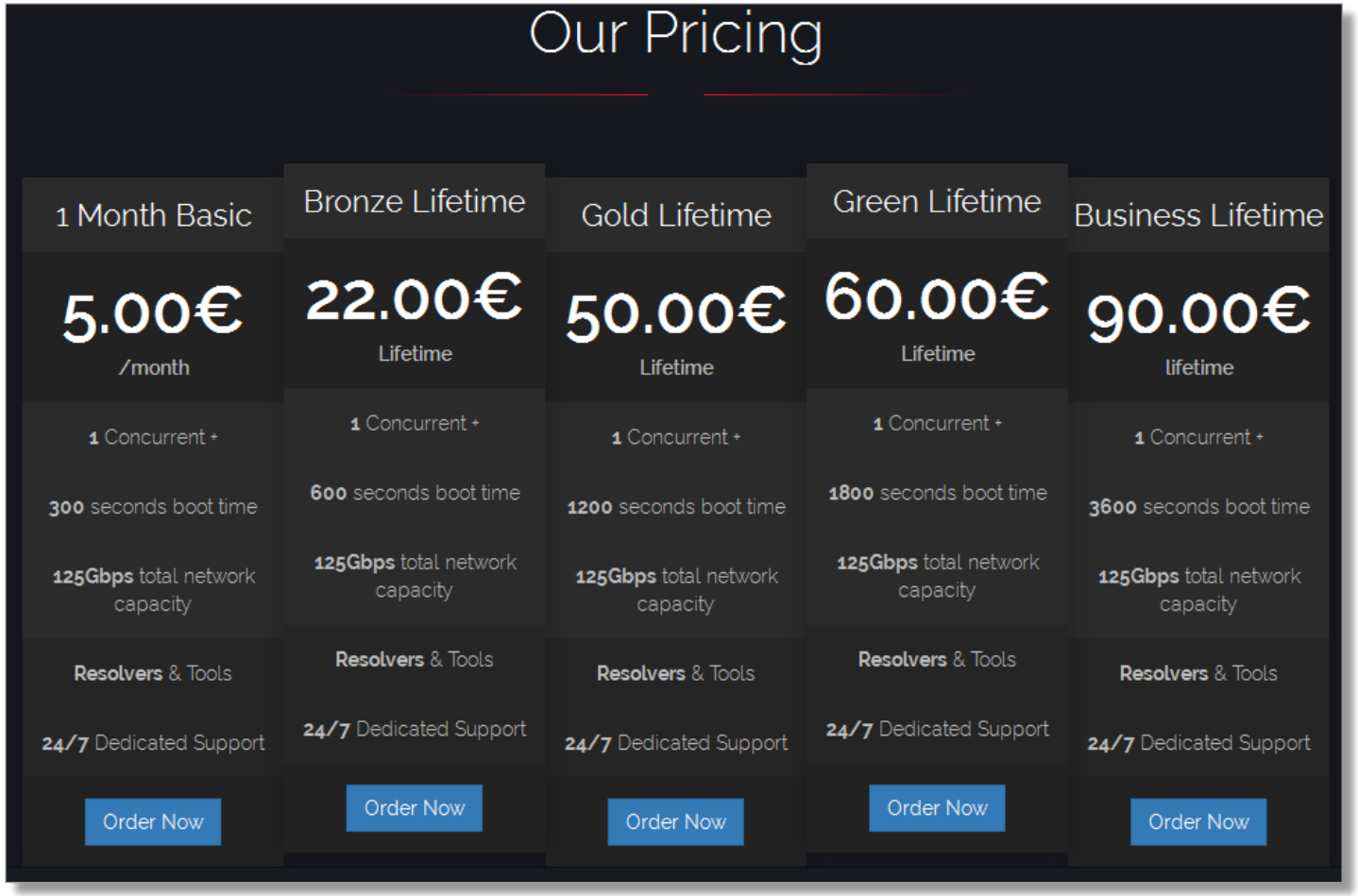
1.2 Tbps

Source: The Hunt for IoT: The Rise of Thingbots, F5 Labs, August 2017

DDoS for Hire

Low sophistication, high accessibility

- **Accessible**
  Booters/stressers easy to find
- **Lucrative**
  Profit margins of up to 95%
- **Effective**
  Many DDoS victims pay up

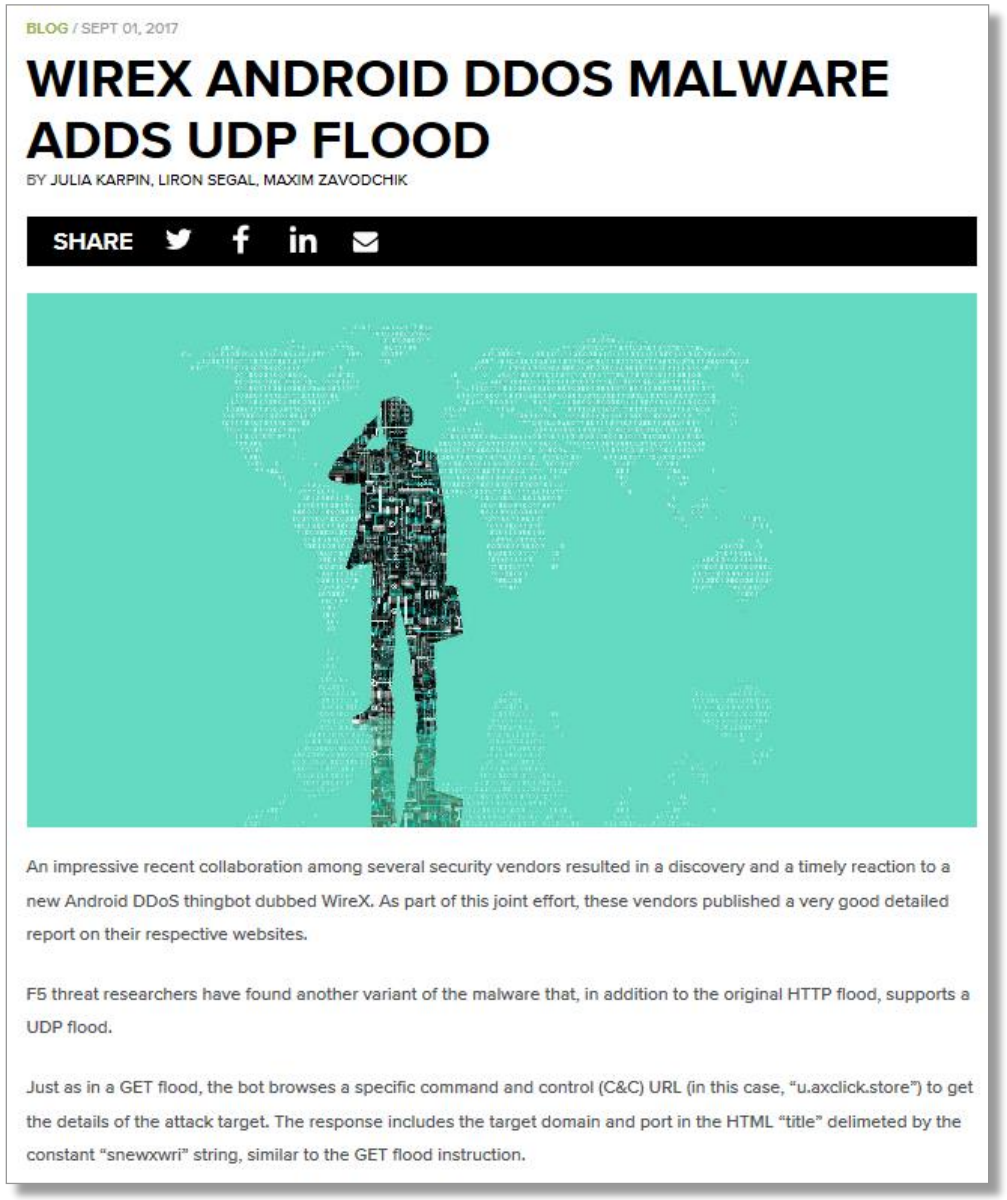


Source: Securelist, Kaspersky Lab, March 2017

DDoS Malware

Application Threat Intelligence

Critical info on threat source and attack type trends



BLOG / SEPT 01, 2017

WIREX ANDROID DDOS MALWARE ADDS UDP FLOOD

BY JULIA KARPIN, LIRON SEGAL, MAXIM ZAVODCHIK

SHARE

An impressive recent collaboration among several security vendors resulted in a discovery and a timely reaction to a new Android DDoS thingbot dubbed WireX. As part of this joint effort, these vendors published a very good detailed report on their respective websites.

F5 threat researchers have found another variant of the malware that, in addition to the original HTTP flood, supports a UDP flood.

Just as in a GET flood, the bot browses a specific command and control (C&C) URL (in this case, "u.axclick.store") to get the details of the attack target. The response includes the target domain and port in the HTML "title" delimeted by the constant "snewxwri" string, similar to the GET flood instruction.

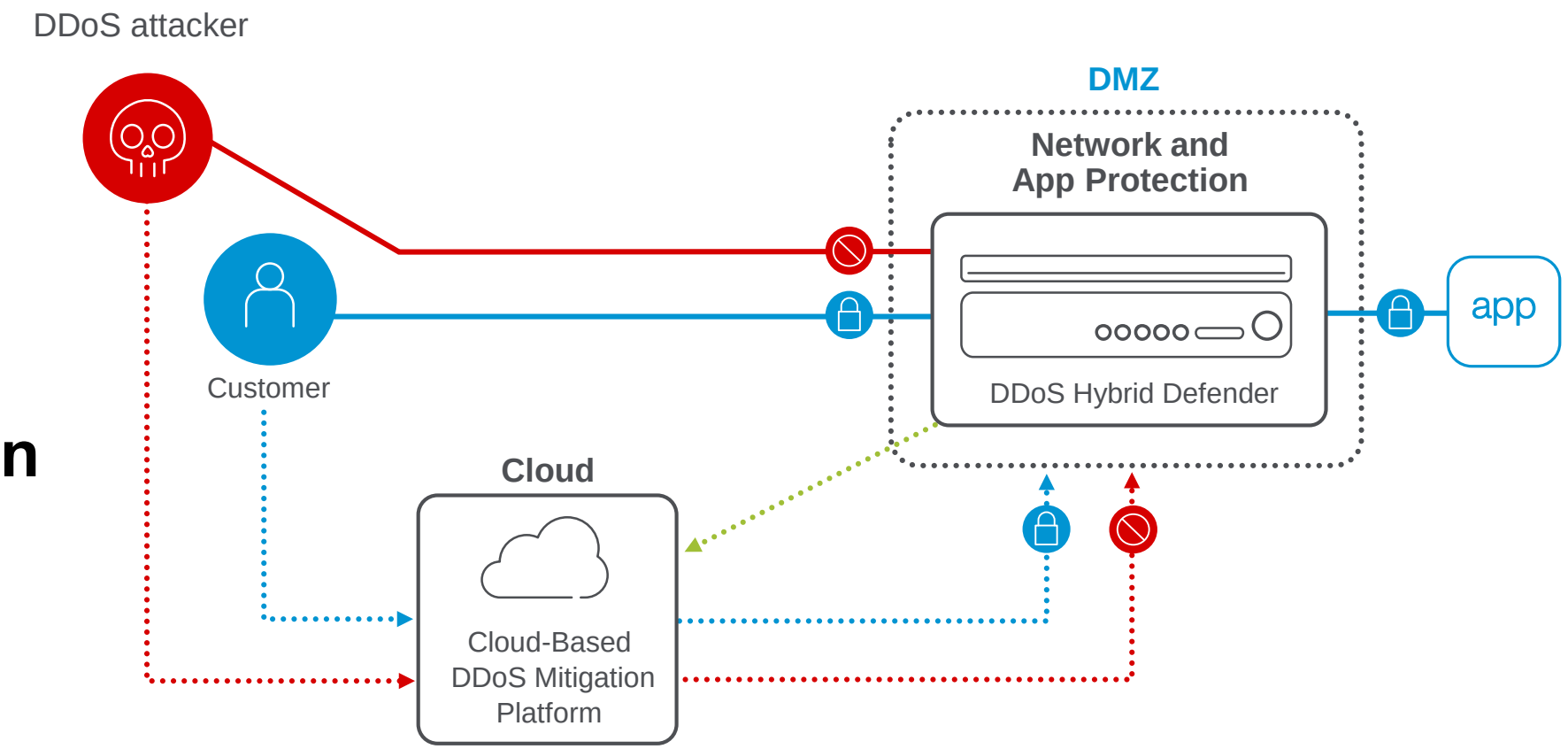
Hybrid DDoS Protection

PROBLEM

DDoS attacks

SOLUTION

DDoS protection with cloud scrubbing



Network Behavioral DDoS

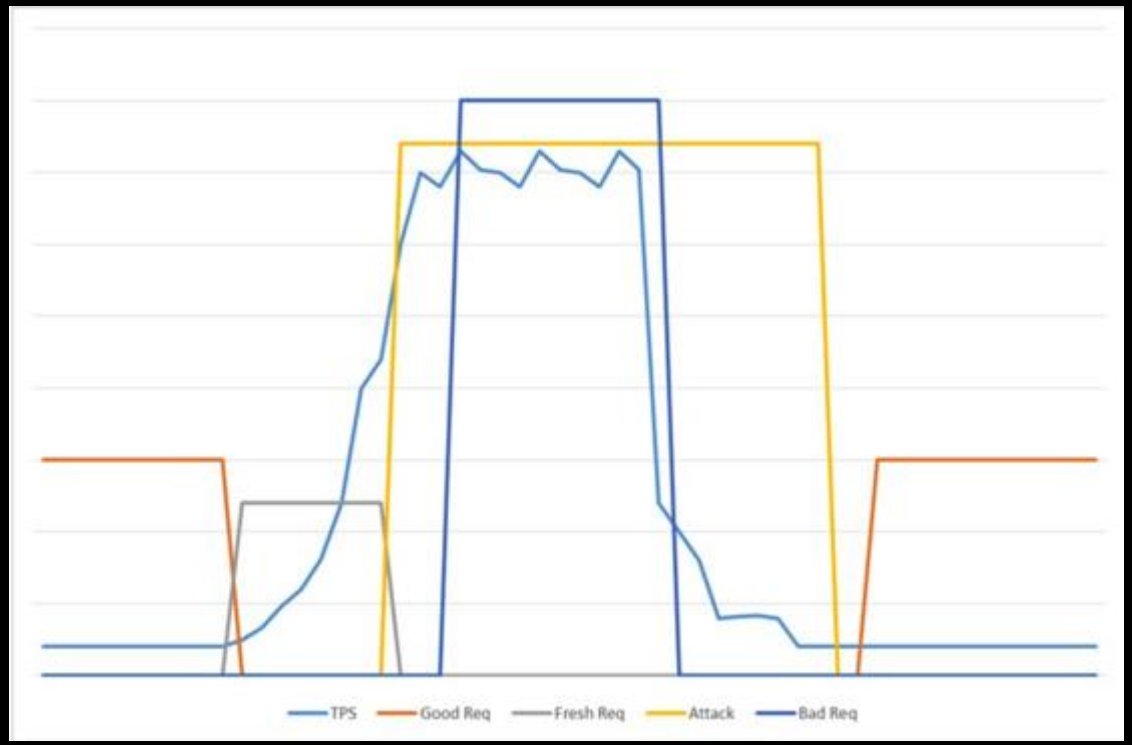
Customer Challenges

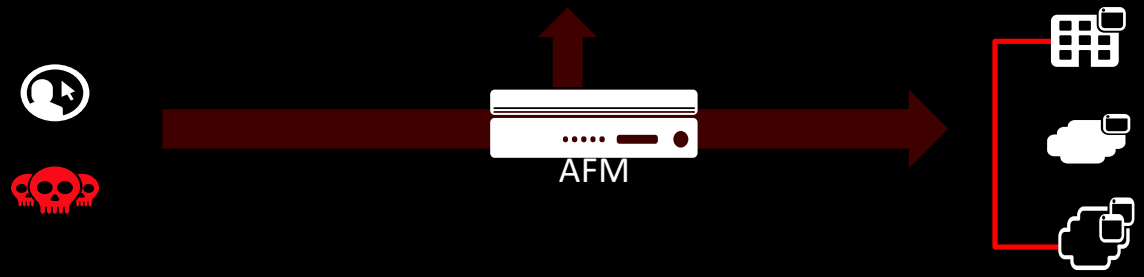
- DDoS attacks are more complex – now multi-vectored
- Detection of complex multi-vectored attacks is limited with static/single dimensional vectors
- Aggregate Rate-limiting “catches” good traffic with bad
- Per-SrcIP ineffective with spoofed IP’s or “wide” botnet attacks

F5 Solution: Network Behavioral DDoS

- Attack detection in both inline and out-of-band deployments
- Sub-second attack detection
- Detects anomalies compared against historical baseline
- Statistical method baselines 3,000+ L3/4 metrics
- Dynamically generates “signatures” (vectors) upon attack detection
- On-demand/real-time “signature” creation and sharing
- Targeted “signatures” = Low false positive rate
- Detect-only mode allows review before enforcement

Monitor and Baseline L3/L4





Per-App (VS) Auto-Thresholding and SrcIP Awareness

Customer Challenges

- Administrators have difficulty determining correct static thresholds for DDoS
- Normal traffic patterns change as applications evolve and administrators are unable to keep up
- There is difficulty in distinguishing between “good guys” (legitimate traffic) and “bad actors” (threats)

F5 Solution: Per-App Auto-Thresholding

- Computes thresholds automatically for all 120+ DDoS vectors or only selected vectors
- Thresholds are continuously adjusted based on changes in traffic patterns
- “What-If” mode available, with report-only and no drops
- Per-SrcIP awareness available on every vector
- Significantly reduces human involvement and errors resulting in greater DDoS accuracy and lower operational impact

L7 DDoS Threshold Auto-Tuning

Customer Challenges

- Determining appropriate DDoS thresholds is difficult
- Ensuring DDoS threshold accuracy as traffic patterns change is a challenge

F5 Solution: L7 DDoS Threshold Auto-Tuning

- Simplifies DDoS threshold settings configuration
- Safeguards accuracy of DDoS threshold settings as traffic patterns change
- Analyzes measured resource usages and automatically establishes threshold values based on historic normalized traffic behavior
- Thresholds can be automatically established per DeviceID, Source IP, URL and site wide, automatically adjusting to continuously strengthen attack responses
- Drives efficiency, accuracy and control
- Strengthens defense policies for greater application protection

L7 Behavioral Analysis DoS

- Starting with BIG-IP ASM v13.1 the ability to create multiple DoS profiles with different BADOS behavior in the policies is now supported on HTTP Profiles

- Different DoS profiles with different BADOS settings can be applied across different hostnames on the same VS

- VS + Profile have now independent BADOS behavior

L7 Behavioral DDOS Protection: an advanced, phased approach

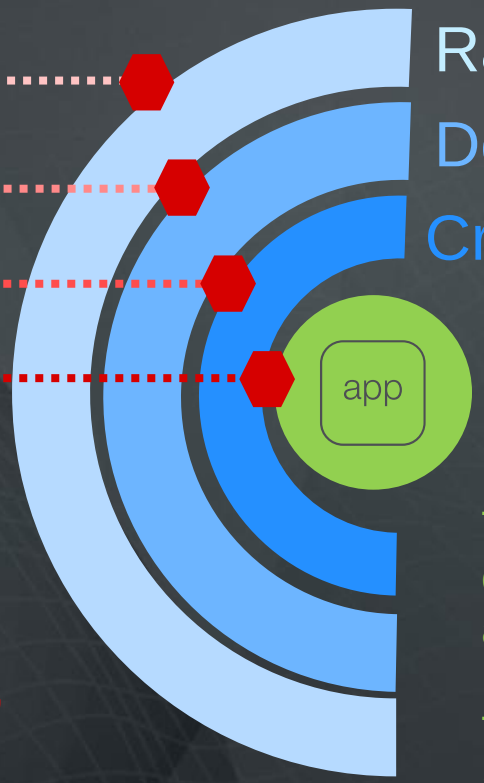
Multiple Layers of Protection

Start of Attack

Identify Attackers

Advanced Attacks

Persistent Attacks



Rate Limit to Protect the Server

Detect and Block Bots and Bad Actors

Create and Enforce Dynamic Signatures

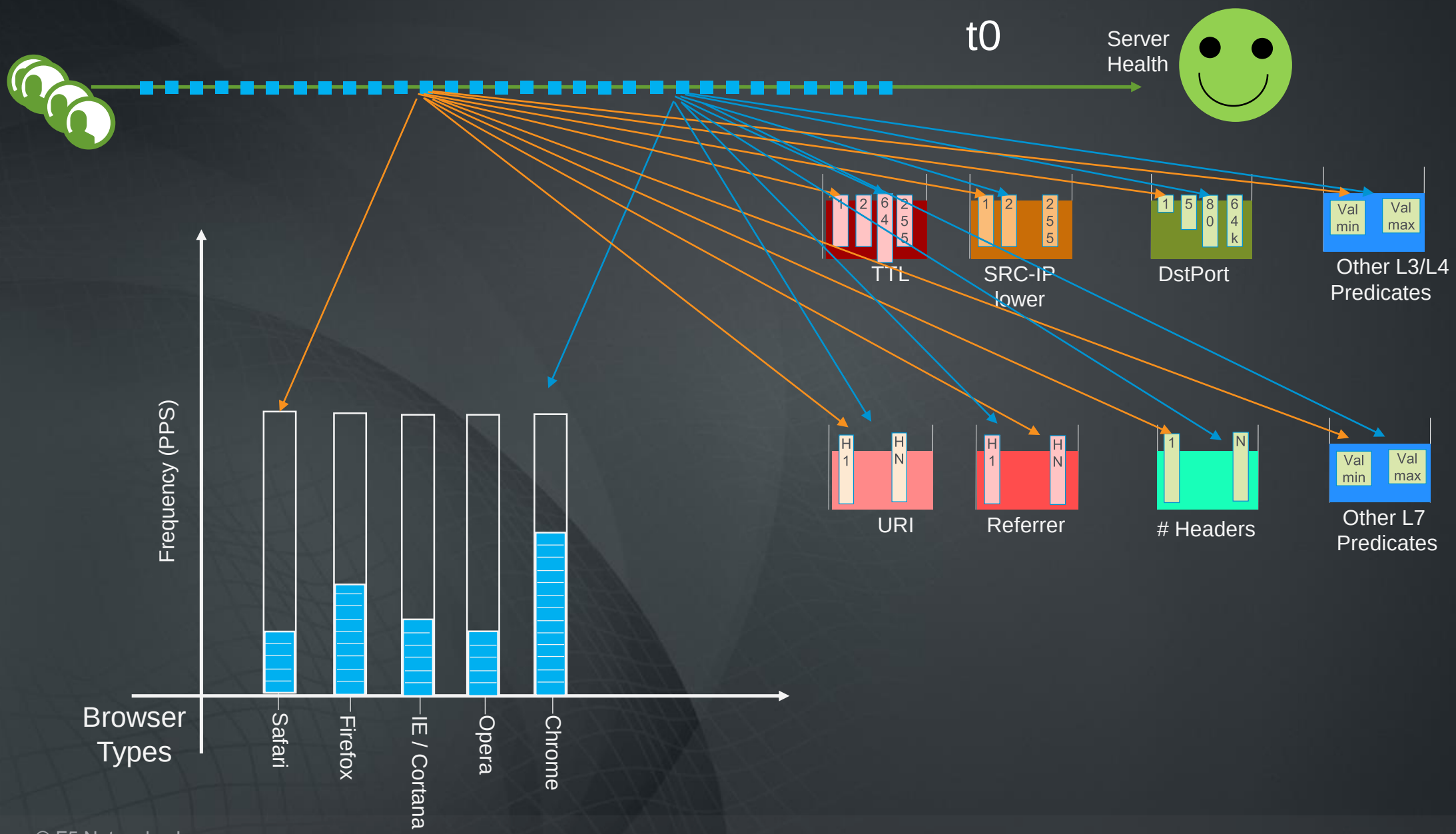
Analyze Application Stress and Continually Tune Mitigations.

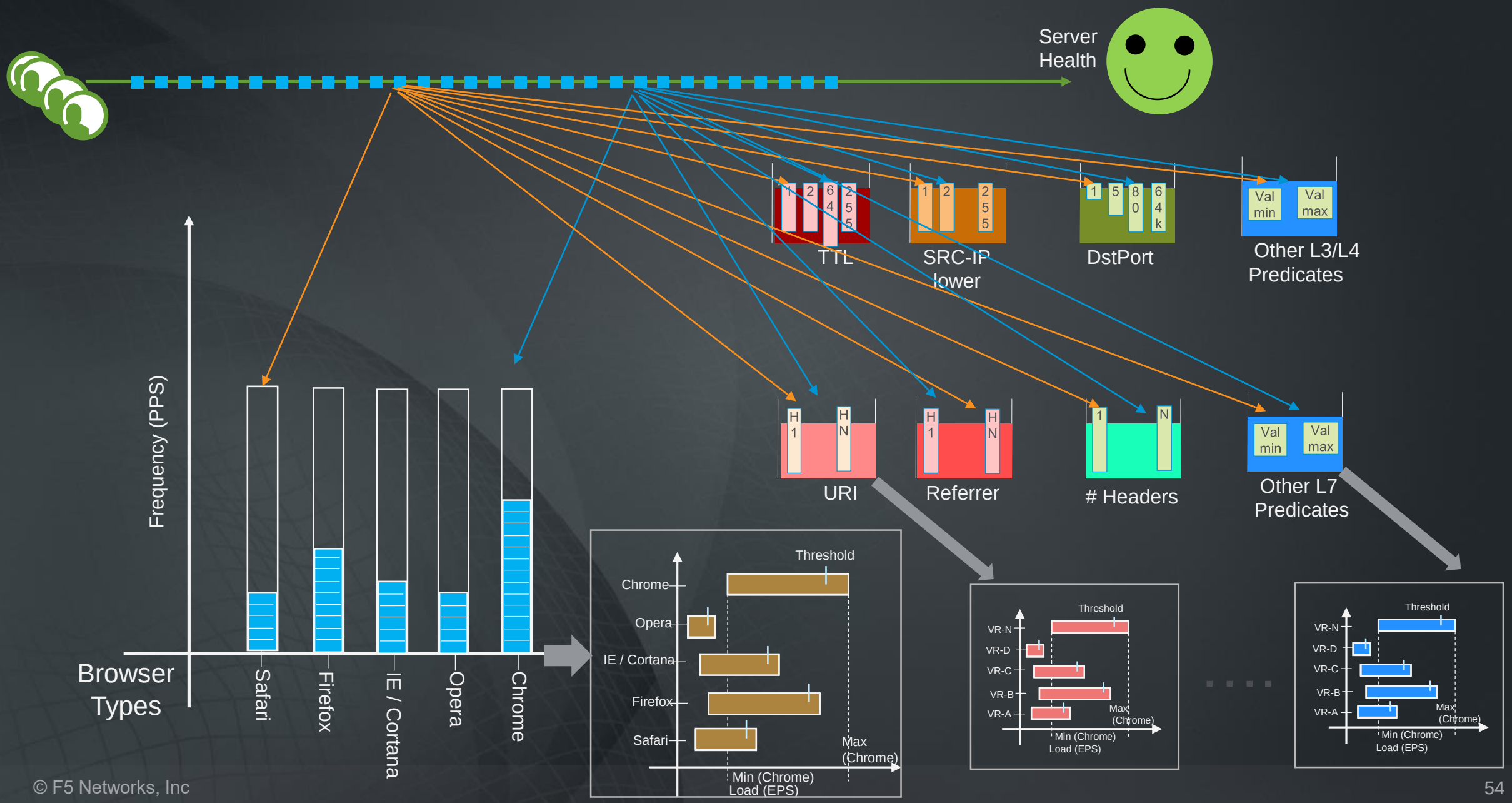
Even basic attacks can take an unprotected server down quickly.

Persistent attackers will adjust tools, targets, sources and attack volume to defeat static DOS defenses.

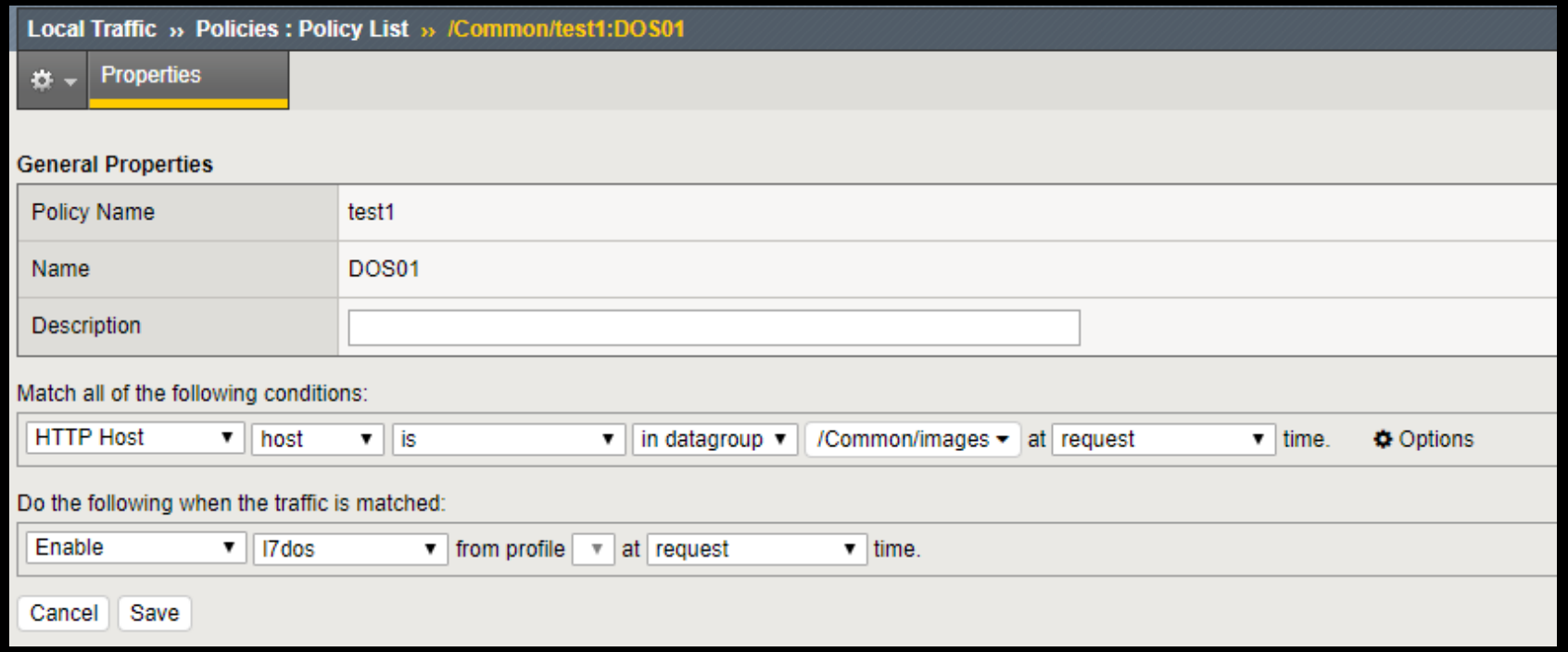
The f5 approach protects the server from the first moment of the attack and then analyzes the attack tools, sources and patterns to refine mitigations.

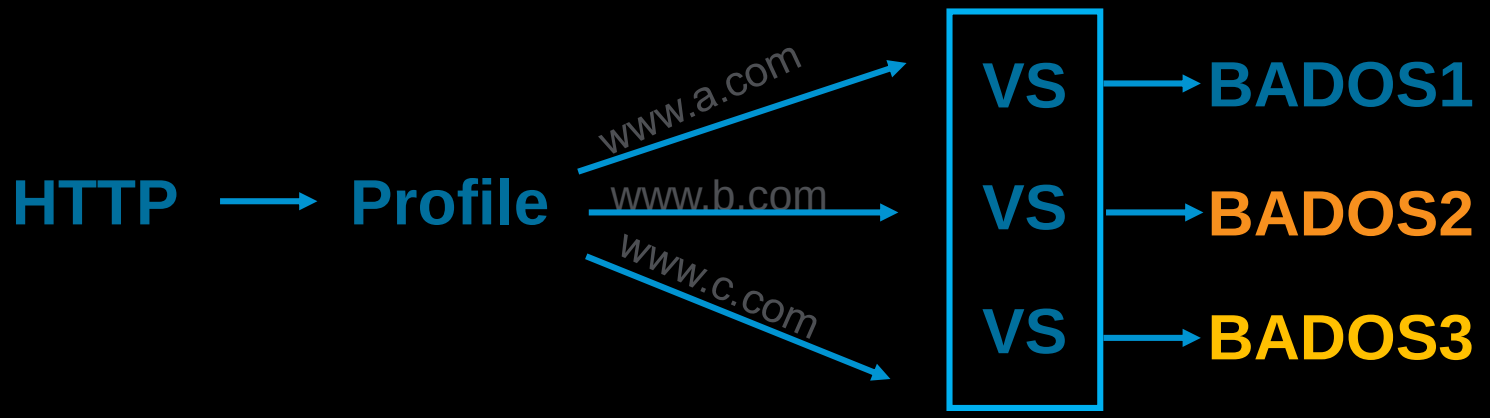
These sophisticated protections maximize application availability while minimizing false positives.





Behavioral Analysis DoS





MALWARE

Malware Trends

In the first quarter of 2017, a new specimen of malware emerged every 4.2 seconds

1 in every 131 emails included malware in 2016

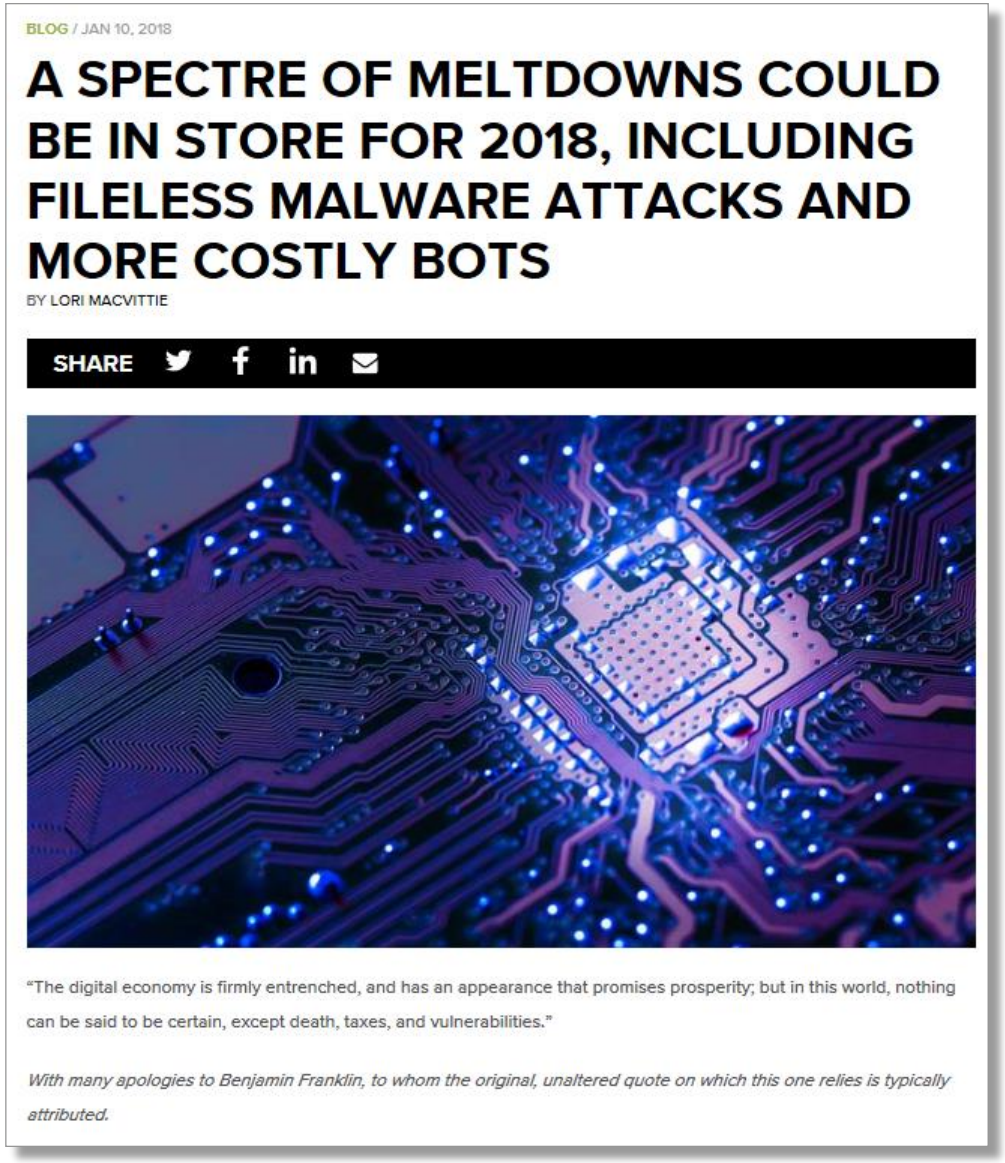
Over half (51%) of all breaches in 2016 involved some form of malware

Sources:
1) Malware trends 2017, G DATA Software
2) Symantec Internet Security Threat Report, April 2017
3) WannaCry Update, Rapid7 Blog, May 2017

Malware Attacks

Application Threat Intelligence

Use our research to learn about new types of malware



BLOG / JAN 10, 2018

A SPECTRE OF MELTDOWNS COULD BE IN STORE FOR 2018, INCLUDING FILELESS MALWARE ATTACKS AND MORE COSTLY BOTS

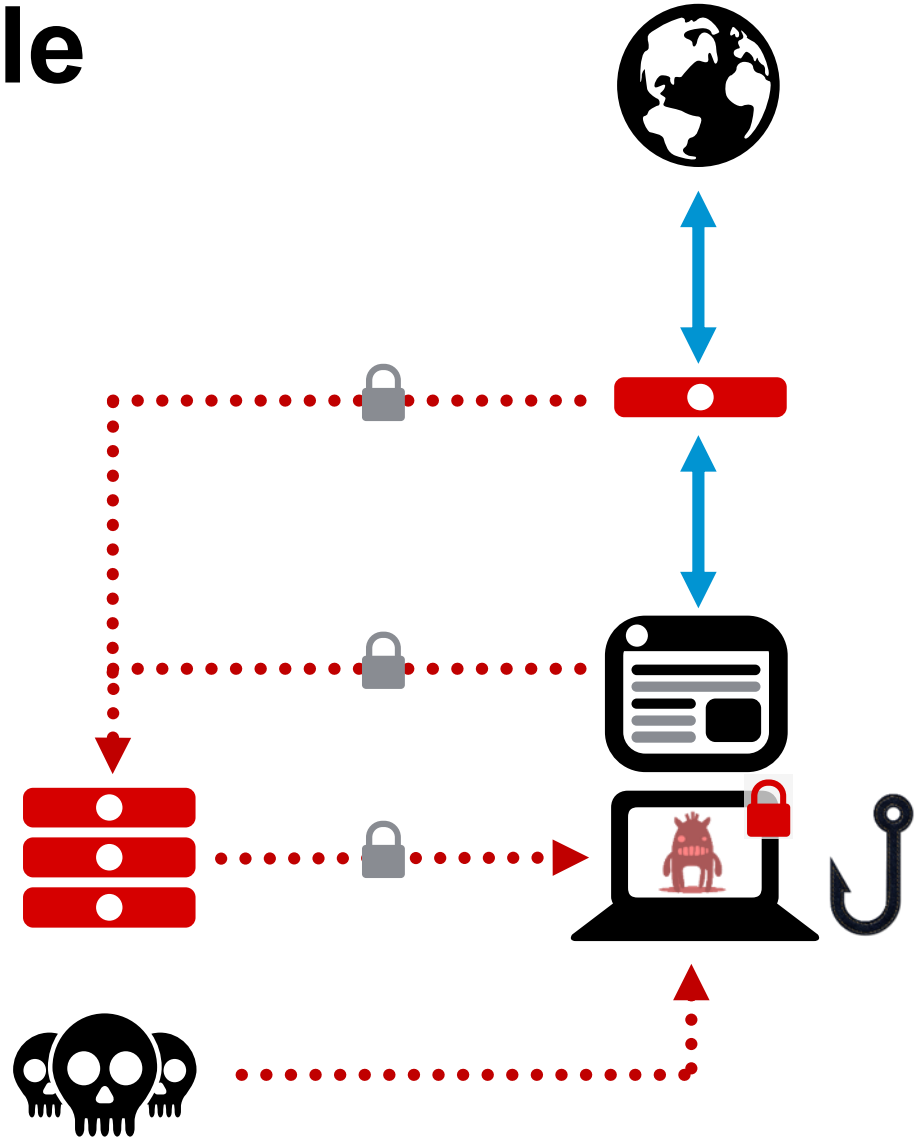
BY LORI MACVITTIE

SHARE

"The digital economy is firmly entrenched, and has an appearance that promises prosperity; but in this world, nothing can be said to be certain, except death, taxes, and vulnerabilities."

With many apologies to Benjamin Franklin, to whom the original, unaltered quote on which this one relies is typically attributed.

MitB Example



MitM – sends credentials to command and control center

Injects into running processes

Hooks functions inside Windows DLLs

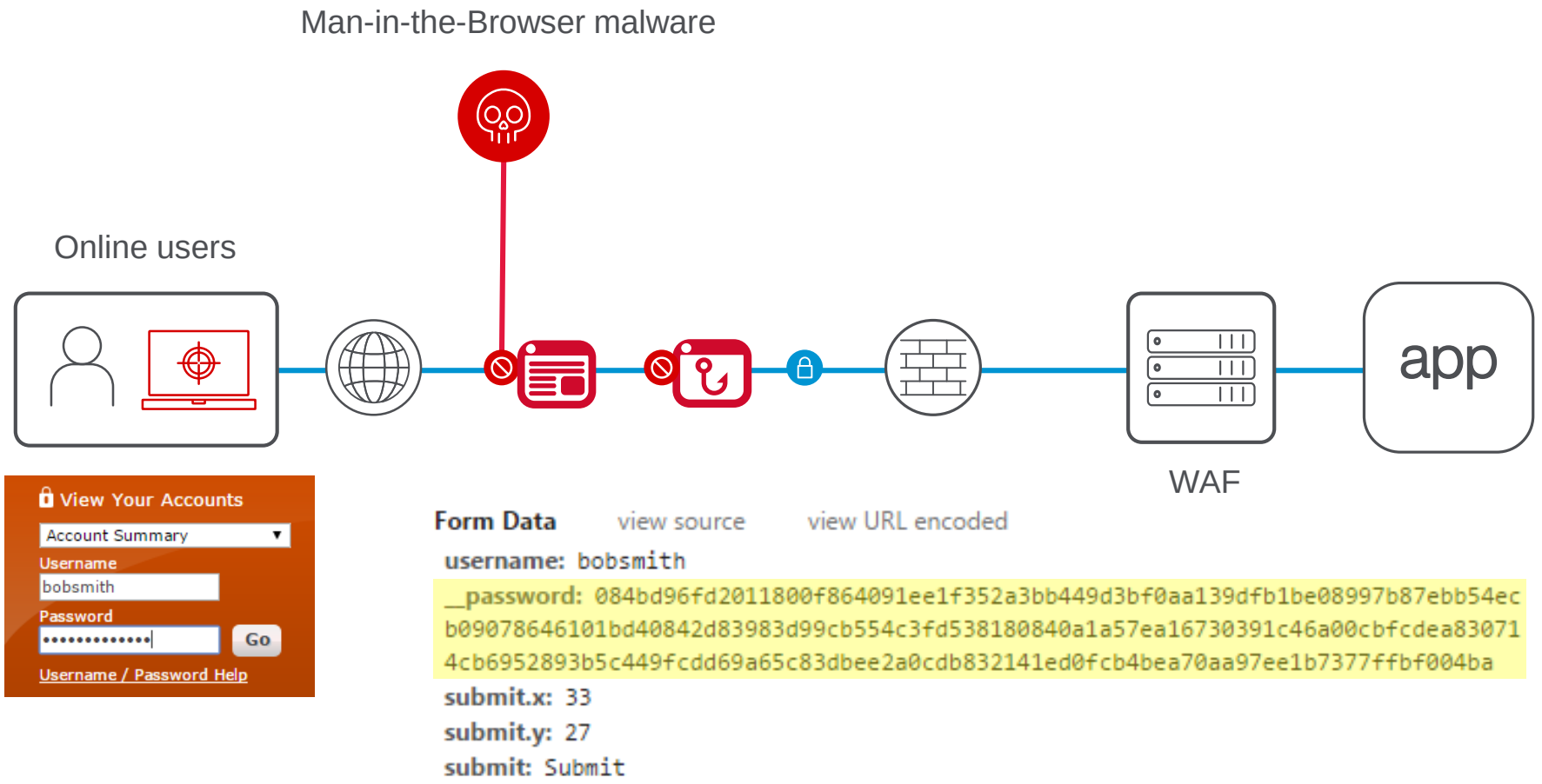
Credential Theft Using Malware

PROBLEM

Malware

SOLUTION

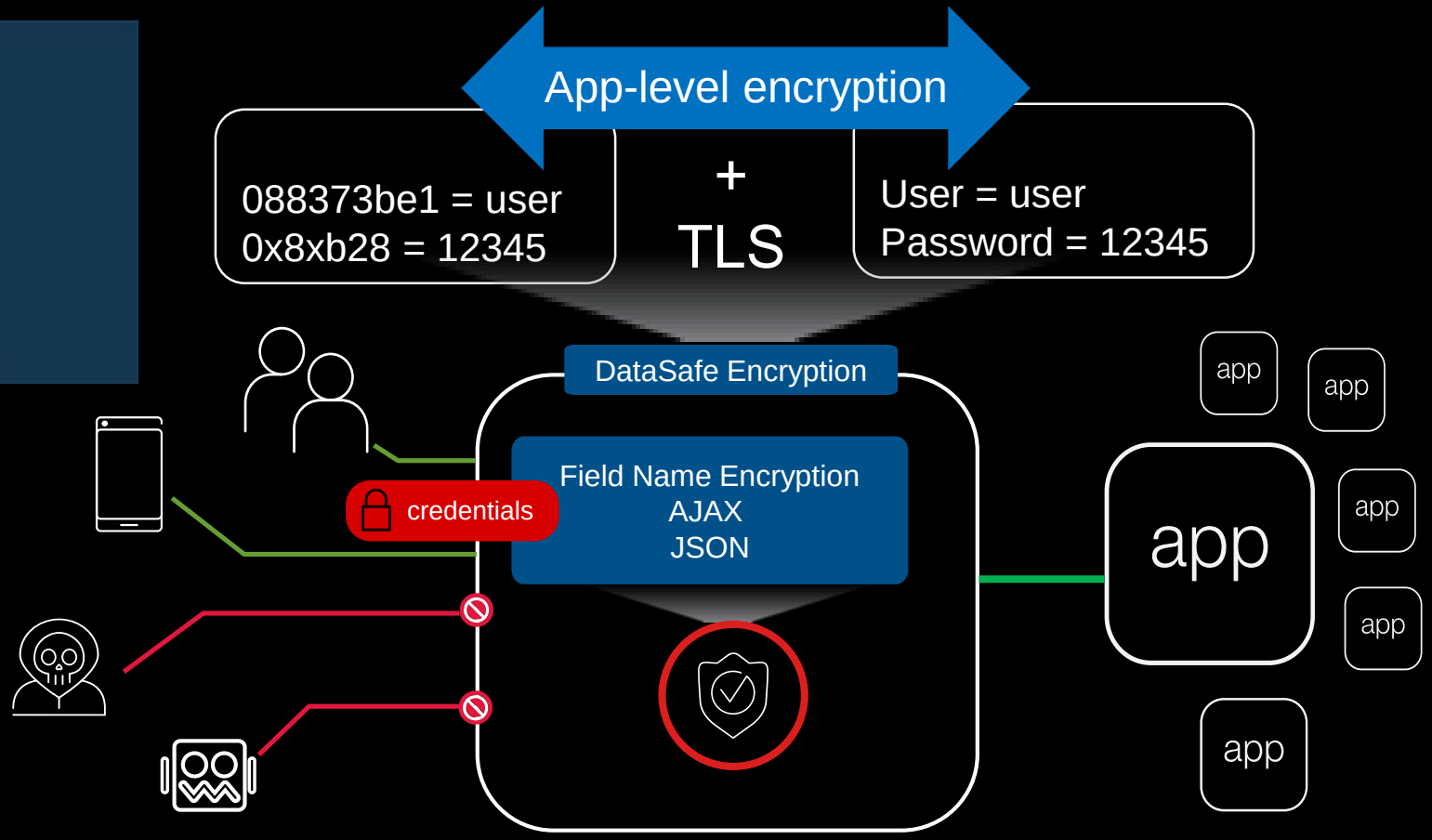
App-layer encryption



Deep Dive: Prevent Data & Credential Theft with F5 DataSafe

No Client or Impact to users

Goes beyond TLS/SSL



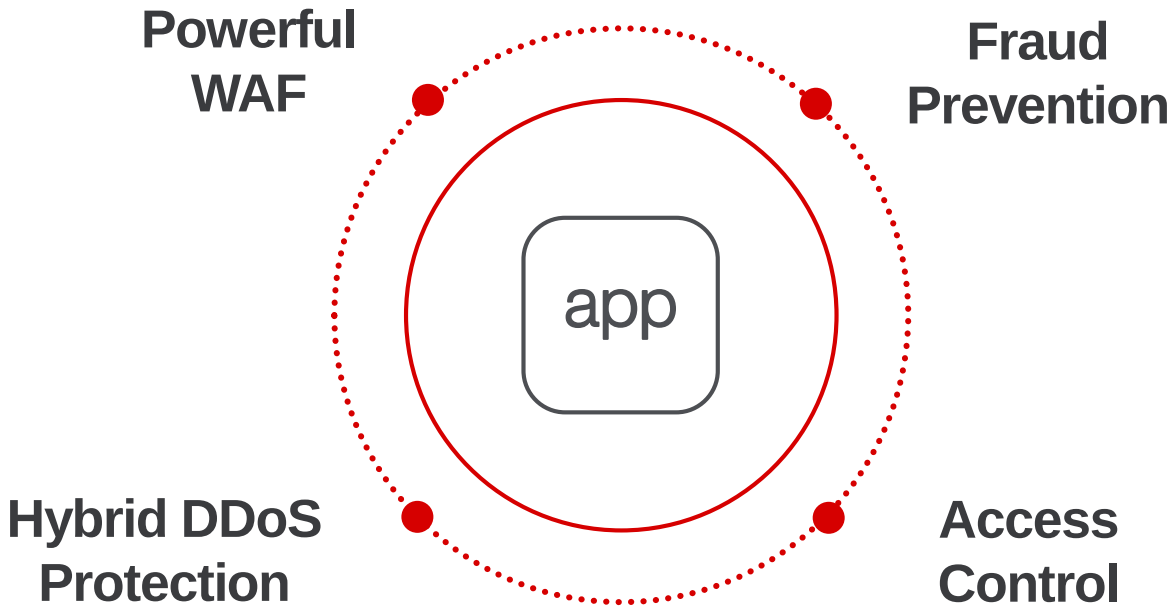
- Perpetual license
- Included in Advanced WAF
- Available as Add-on

Stolen credential cannot be re-used

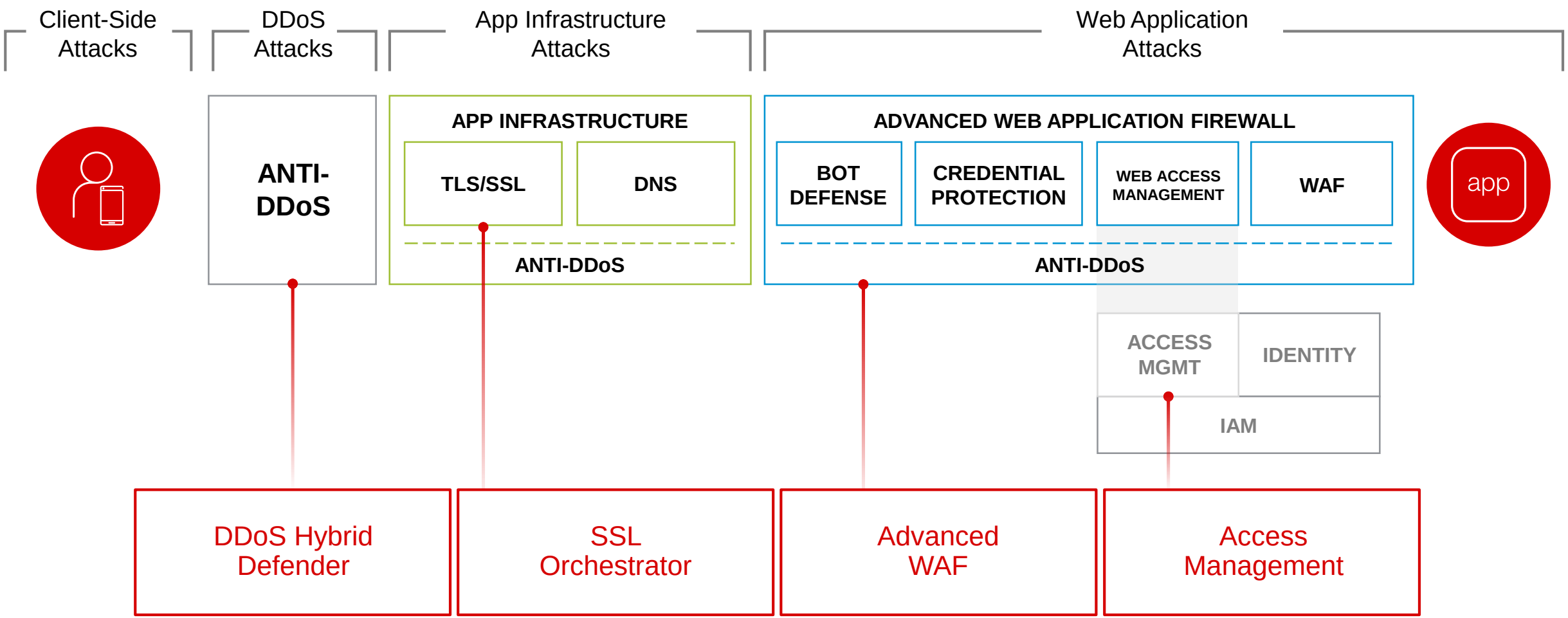
No app updates required

SUMMARY

App-Centric Security

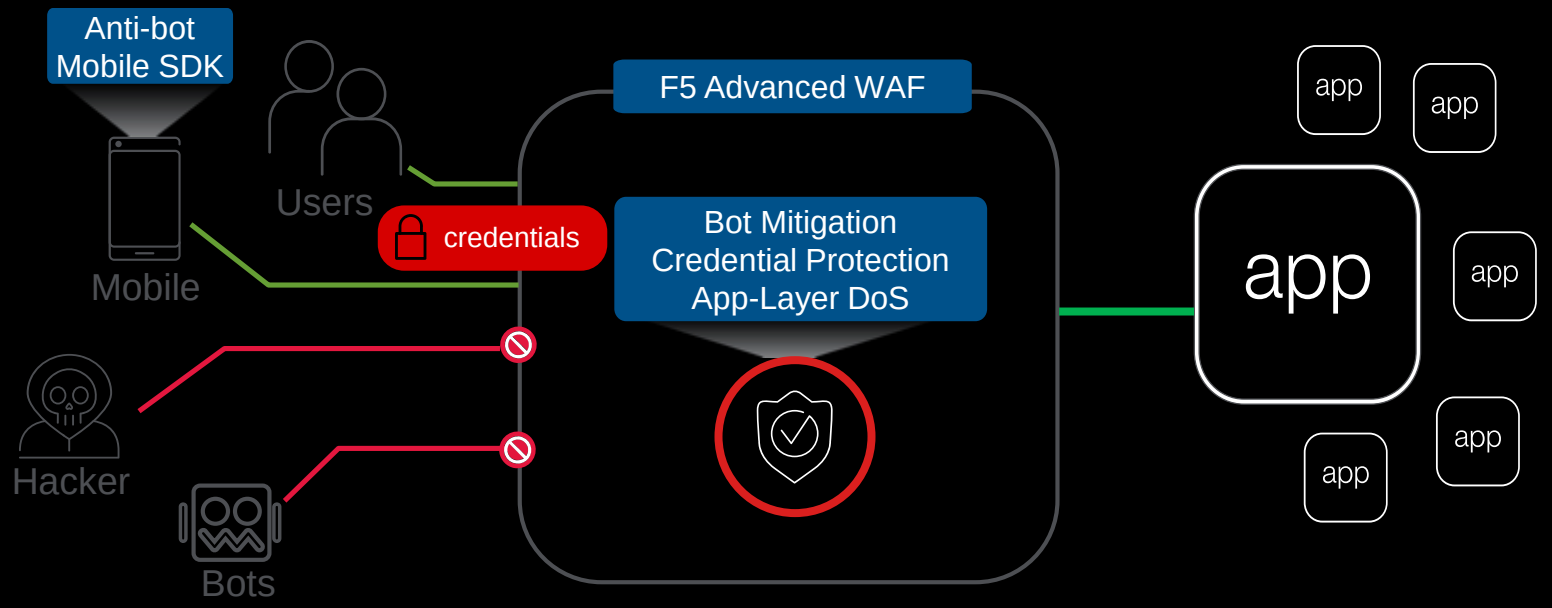


App Protection Framework



F5 Advanced WAF

Protect against bots, credential attacks, and app-layer DoS



Defend against bots

- Proactive bot defense
- Anti-bot mobile SDK
- Client and server monitoring

Prevent Account Takeover

- App-level encryption
- Mobile app tampering
- Brute Force protection

Protect apps from DoS

- Auto-tuning
- Behavioral analytics
- Dynamic signatures

Key Benefits:

- Protects Web and mobile apps from exploits, bots, theft, app-layer DoS
- Prevent malware from stealing data and credentials
- Prevent Brute Force attacks that use stolen credentials
- Eliminate time-consuming manual tuning for App-layer DoS protection

F5 Advanced WAF Competitive Advantage

Key F5 Advantages

- ✓ Bot Protection
- ✓ Account Takeover
- ✓ App-Layer DoS

Bot protection beyond signatures and reputation

- ✓ Web and mobile app protection
- ✓ Client fingerprinting
- ✓ Server performance monitoring

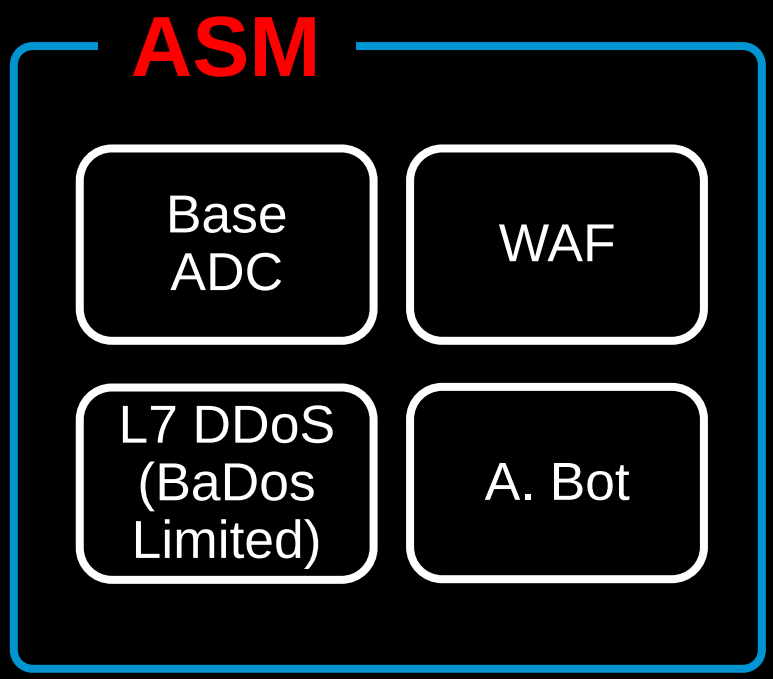
Account Takeover that stops credential theft and abuse

- ✓ Application Layer Encryption
- ✓ Obfuscation and evasion detection
- ✓ Comprehensive Brute Force mitigation

App-Layer DoS that adapts to changing apps

- ✓ Real-time application baselines
- ✓ Behavioral analysis with machine learning
- ✓ Dynamic signatures with low false positives

ASM today (simplified)



Feature List per Product Offering

F5 Advanced WAF

- Base ADC
- WAF
- L7 DDoS
- A. Bot
- A. Bot Mobile SDK (Reduced price) **($)**
- (I) Data safe
- (I) BaDoS Unlimited
- (I) Upstream Signaling (soon)

ASM

- Base ADC
- WAF
- L7 DDoS (BaDos Limited)
- A. Bot
- A. Bot Mobile SDK **($)**

($) - Add On

(I) – Included in the AWAF

SOLUTIONS FOR AN APPLICATION WORLD