Application Protection Sales Play

Hybrid Web Application Firewall

Hybrid WAF Prerequisites

This playbook assumes a basic understanding of BIG-IP ASM and Silverline WAF technologies, use cases, and value, based on existing training materials.

BIG-IP ASM education

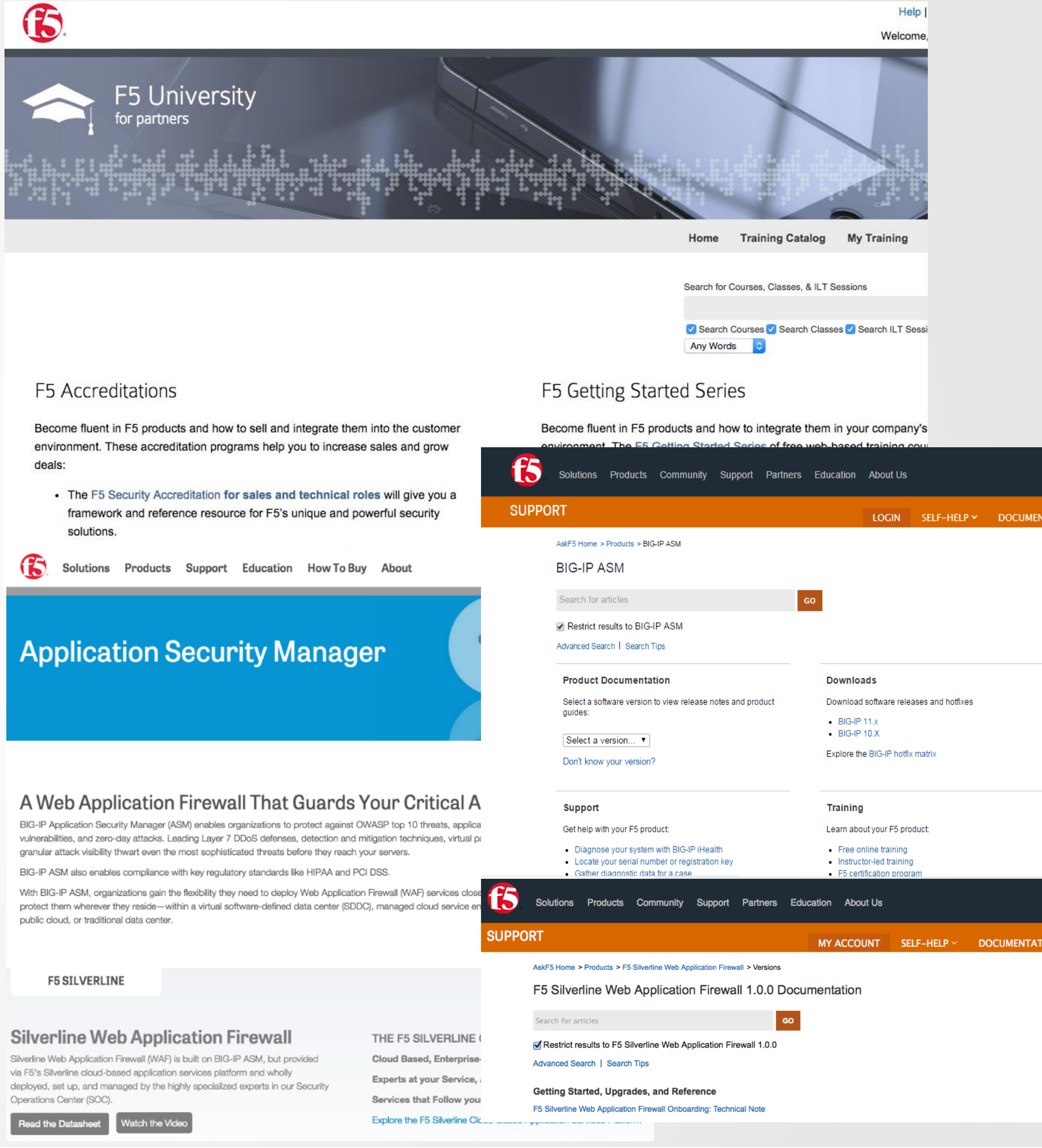
Web based training and product information

- Product Training https://university.f5.com/
- Follow us on f5.com: Application Security Manager
- Manuals and Release Notes on f5.com

Silverline WAF education

Product information

- Follow us on f5.com: Silverline WAF
- Onboarding Tech. Notes on f5.com



Search for Courses, Classes, & ILT Sessions

☑ Search Courses ☑ Search Classes ☑ Search ILT Sessi

Any Words

F5 Accreditations

Become fluent in F5 products and how to sell and integrate them into the customer environment. These accreditation programs help you to increase sales and grow deals:

- The F5 Security Accreditation for sales and technical roles will give you a framework and reference resource for F5's unique and powerful security solutions.

F5 Getting Started Series

Become fluent in F5 products and how to integrate them in your company's environment. The F5 Getting Started Series of free web-based training cou

Application Security Manager

A Web Application Firewall That Guards Your Critical A

BIG-IP Application Security Manager (ASM) enables organizations to protect against OWASP top 10 threats, applica vulnerabilities, and zero-day attacks. Leading Layer 7 DDoS defenses, detection and mitigation techniques, virtual pa granular attack visibility thwart even the most sophisticated threats before they reach your servers.

BIG-IP ASM also enables compliance with key regulatory standards like HIPAA and PCI DSS.

With BIG-IP ASM, organizations gain the flexibility they need to deploy Web Application Firewall (WAF) services close protect them wherever they reside—within a virtual software-defined data center (SDDC), managed cloud service en public cloud, or traditional data center.

F5 SILVERLINE

Silverline Web Application Firewall

Silverline Web Application Firewall (WAF) is built on BIG-IP ASM, but provided via F5's Silverline cloud-based application services platform and wholly deployed, set up, and managed by the highly specialized experts in our Security Operations Center (SOC).

THE F5 SILVERLINE

Cloud Based, Enterprise-

Experts at your Service,

Services that Follow you

Explore the F5 Silverline Cl

AskF5 Home > Products > BIG-IP ASM

BIG-IP ASM

Search for articles

☑ Restrict results to BIG-IP ASM

Advanced Search | Search Tips

Product Documentation

Select a software version to view release notes and product guides:

Select a version...

Don't know your version?

Downloads

Download software releases and hotfixes

- BIG-IP 11.x
- BIG-IP 10.X

Explore the BIG-IP hotfix matrix

Support

Get help with your F5 product:

- Diagnose your system with BIG-IP iHealth
- Locate your serial number or registration key
- Gather diagnostic data for a case

Training

Learn about your F5 product:

- Free online training
- Instructor-led training
- F5 certification program

AskF5 Home > Products > F5 Silverline Web Application Firewall > Versions

F5 Silverline Web Application Firewall 1.0.0 Documentation

Search for articles

☑ Restrict results to F5 Silverline Web Application Firewall 1.0.0

Advanced Search | Search Tips

Getting Started, Upgrades, and Reference

F5 Silverline Web Application Firewall Onboarding: Technical Note

Topics To Drive Hybrid WAF Wins

TOPIC	
Make More Money Selling Hybrid WAF!	
WAF Market And Customer Challenges	
Rethink Security Architectures with App Perimeter	
Identify Hybrid WAF Opportunities	
Selling Hybrid WAF	
Selling Silverline WAF	
Winning With Hybrid WAF	
How Customers Buy F5	

Note: You should be trained already in BIG-IP ASM/Silverline WAF

Who Is This Playbook For?

- MAMs
- TAMs
- ATAMs
- CAMs
- SPMs
- PSMs
- ITAMs
- ISAMs

How Does This Playbook Help?

- Communicates sales best practices and describes what the salesperson should do in different situations they might encounter when selling the product.
- Help new salespeople coming on board but should not be considered a substitute for sales training.

When To Use?

- Use as a resource for trained salespeople to leverage in recalling best practices in real-time, helping identify where best opportunities are, what impediments to sales success exist, and how to marshal resources and messages to tackle both.

Make More Money Selling Hybrid WAF!

What's In It For You?

- **Expand your business** and sell Hybrid WAF protecting all web apps
- **Increase deal size** of existing DDoS Protection with App Protection (ASM/ Silverline WAF)
- **Set the stage** for future solution offerings tied to the broader security portfolio

Understanding the WAF Market and Customer Challenges

Key Takeaways For Market And Customer Challenges

1. F5 is a recognized challenger in a growing market

2. WAF market growth driven by increases in app attacks, mobility and cloud adoption

3. Protecting applications creates new customer challenges and opportunities for F5

F5: Recognized As Leading Challenger In Growing Market

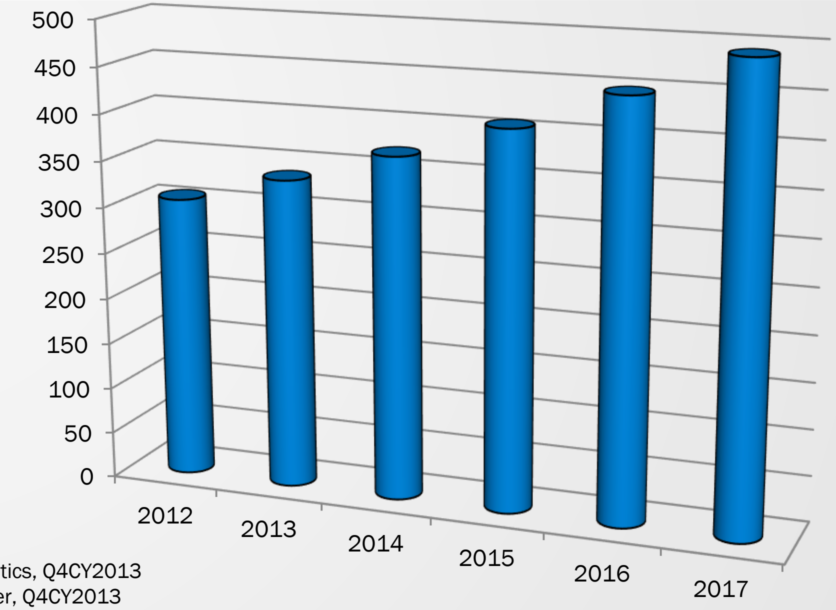
Web Application Firewall (WAF) Market size, Growth and TAM through 2017

Market Growth and Revenue Trends

TAM in 2015 stands at $407M trending toward $492M in 2017

- **WAF market growth from $306 million in 2013 to $500 million by 2018, with a CAGR* of 17.2%**
- Gartner recognized F5 as the leading challenger to Imperva, backed by an unmatched ability to execute
- Largest revenue generating industries: **Banks, Insurance, E-commerce, and Government**
- Over 50% of public web apps will use WAFs delivered as a cloud service or internet-hosted virtual appliance by 2020

WAF Total Addressable Market



- Infonetics, Q4CY2013
- Gartner, Q4CY2013
- IDC, 2013
- Gartner WAF MQ 2014, F5

* Technavio report, titled, "Global Web Application Firewall (WAF) Market 2014-2018 "

WAF Market Growth Driven By Increases In App Attacks

EVERY
23 Mins.
A WEBSITE IS HIT BY A CRITICAL EXPLOIT
F5 Security Research

2.3M Bots
actively attacking
Symantec Internet Security Report 2014

86% *of websites = 1 serious vuln.;*
56 vulnerabilities per website on avg.
WhiteHat Security Statistics Report 2015

89% of IT security budgets increasing
2014 Cyber Defense report, Bluecoat.

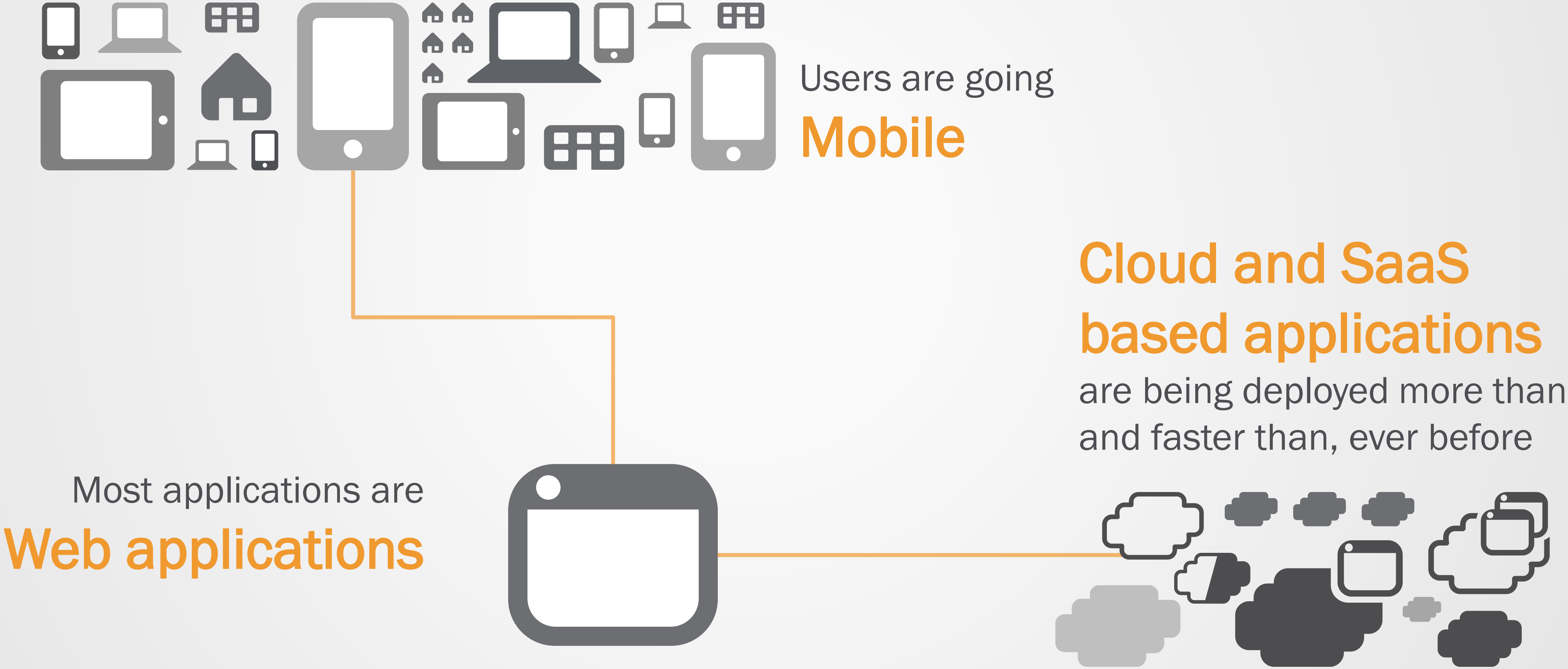
100s
Internet of things emerging
Hundreds of devices and applications introduce attacker exploits

56% employ WAF as part of the security threat defense moving from compliance to security (2015 Cisco Annual Security Report)

<40% have an organized effort for app patching. 2015 Cisco Annual Security Report

36% use **hybrid security** and increasing to 48% over the next couple of years*

Mobility, Cloud Adoption, & App Migration Increase Opportunities



Users are going **Mobile**

Cloud and SaaS based applications are being deployed more than, and faster than, ever before

Most applications are **Web applications**

Application Attacks Hurt Our Customers

Evolving security threats

$1M+ Cost of single cyber attack can be well above $1,000,000

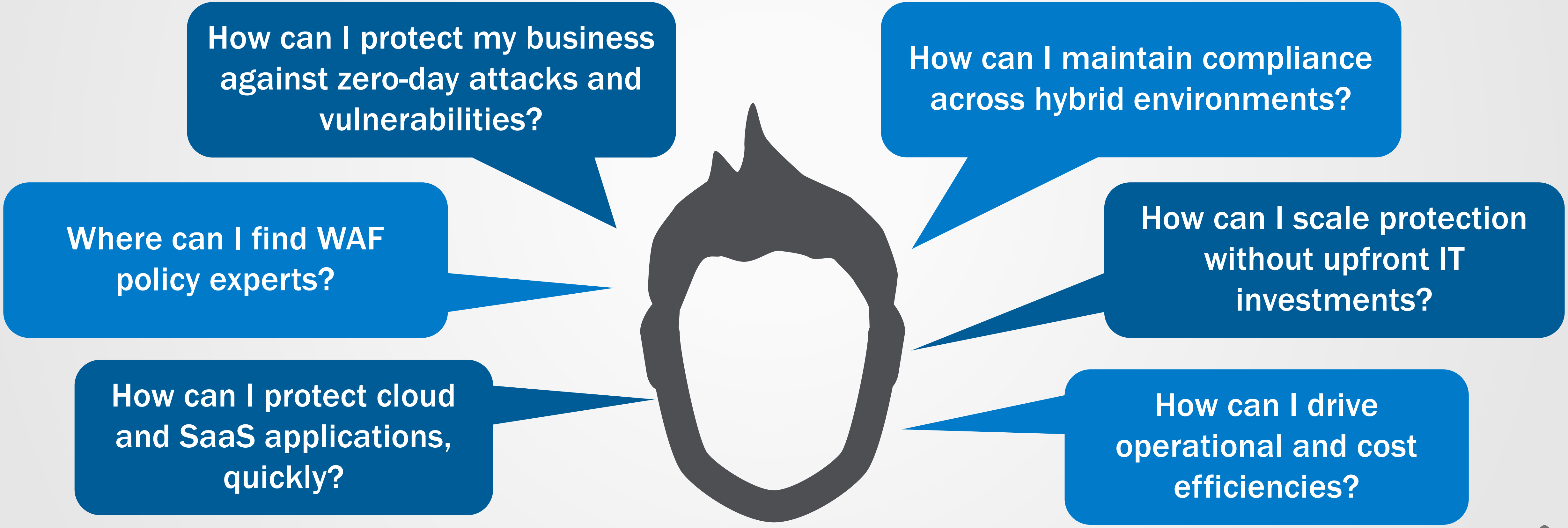
122 Successful attacks per week[1]

1.5M Monitored cyber attacks in US[2]

- Damages brand reputation
- Results in significant downtime and revenue loss
- Compromises sensitive enterprise, employee and customer data
- Breaches compliance required to conduct business online

Source: 1 *Ponemon Institute, Cost of Cyber Crime Study*, 2 *IBM Security Services, 2014 Cyber Security Intelligence Index*

Application Threats Create Customer Challenges And Opportunities For F5



How can I protect my business against zero-day attacks and vulnerabilities?

How can I maintain compliance across hybrid environments?

Where can I find WAF policy experts?

How can I scale protection without upfront IT investments?

How can I protect cloud and SaaS applications, quickly?

How can I drive operational and cost efficiencies?

Rethink Security Architectures with App Perimeter

Key Takeaways For Rethink Security Architectures

1. Understand the new perimeter is an app perimeter

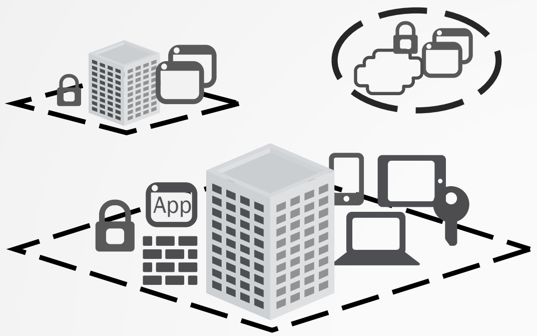
2. F5 architecture is the foundation for defense against advanced threats

3. Security messaging hierarchy helps you recommend the best solutions

The New Perimeter Is An App Perimeter

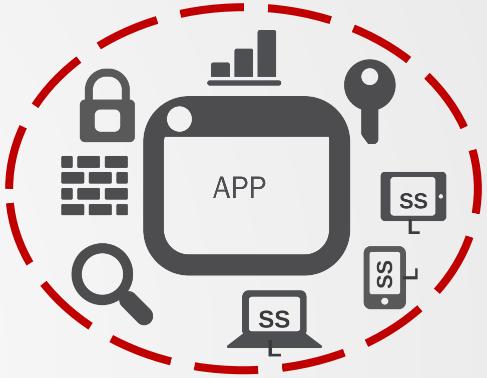
Apps Are The Gateway to Data!

TRADITIONAL



TRADITIONAL NETWORK PERIMETER

F5



PER-APP / PER-USER PERIMETER

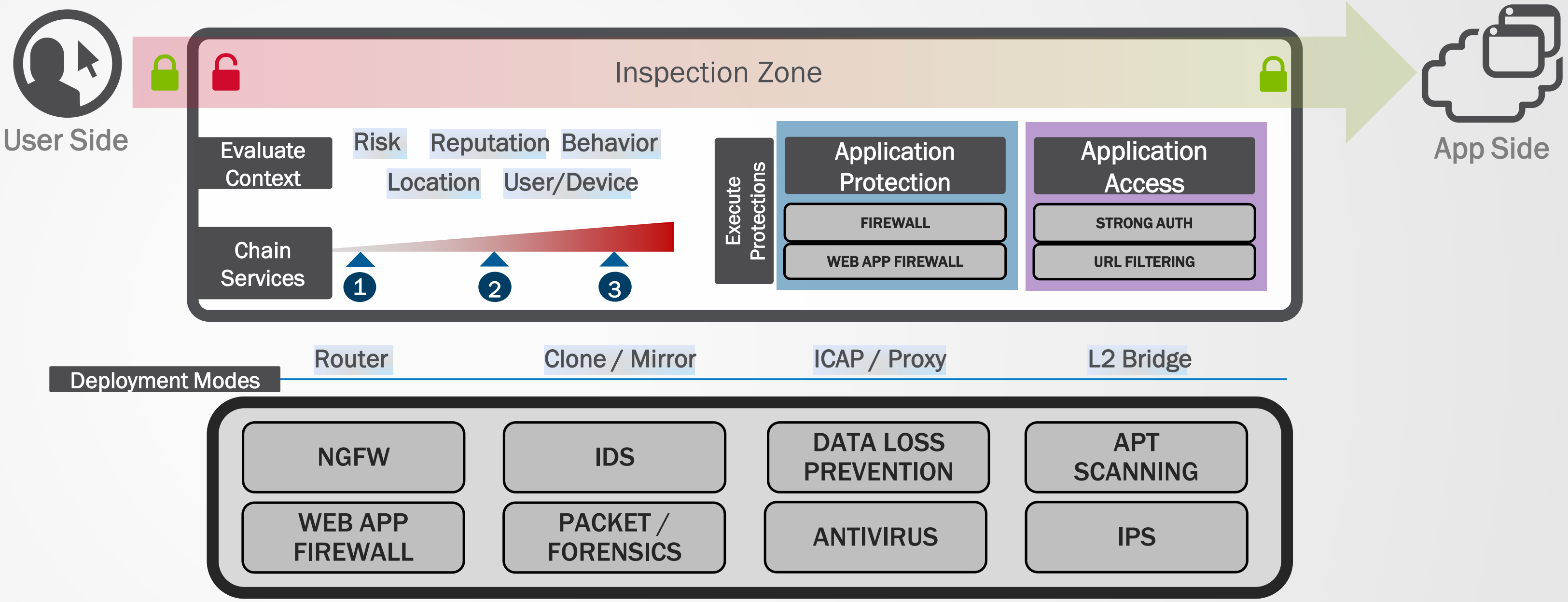
SSL-visible	✗	✓
Location-independent	✗	✓
Session-based	✗	✓
Continuous trust verification	✗	✓
Strategic control points	✗	✓
App availability	✗	✓

IT'S TIME TO RETHINK SECURITY ARCHITECTURES

F5 Architecture For The New Perimeter

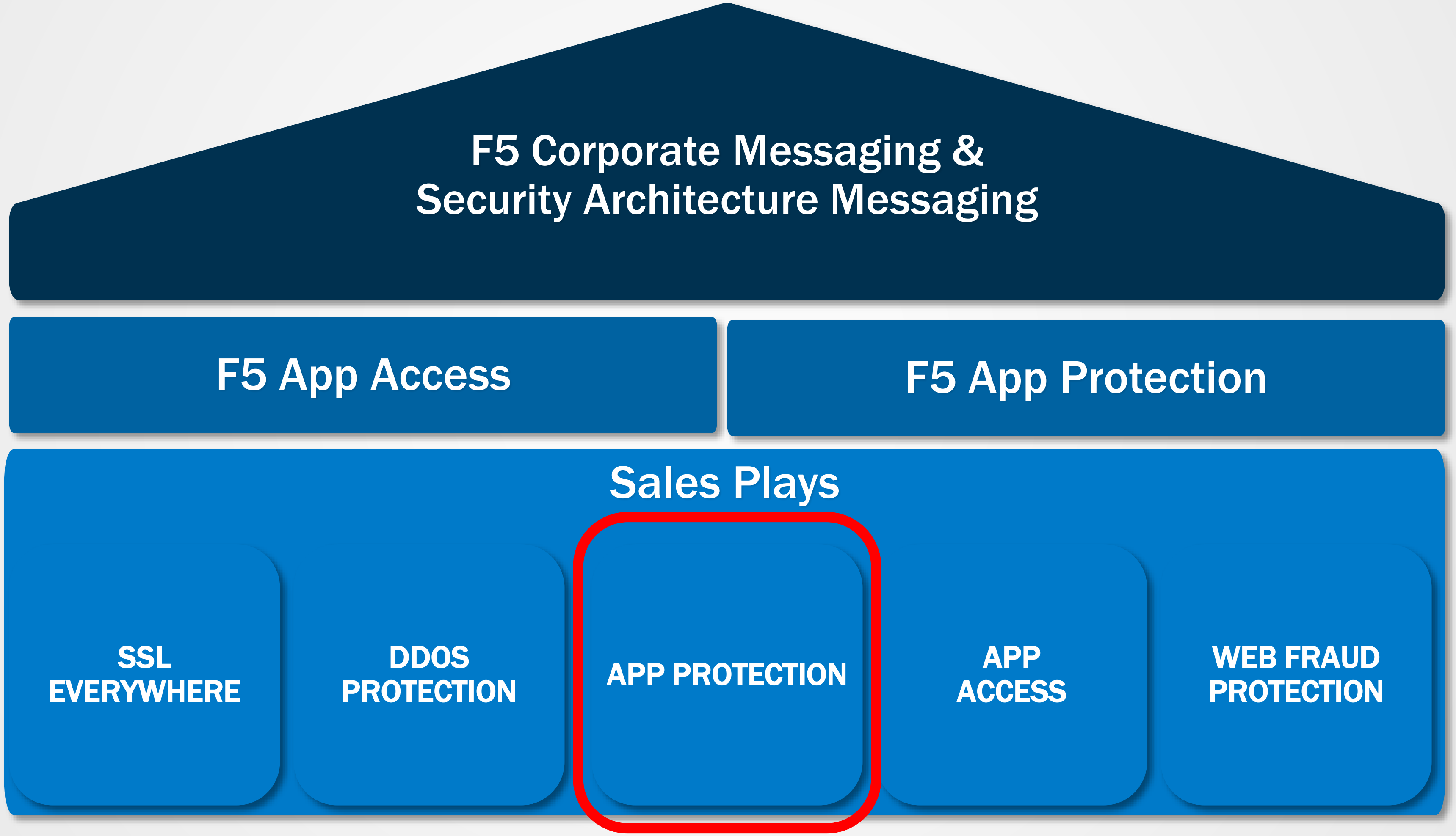
Full Proxy defense against advanced security threats

- Evaluate Context
  - User, device, location, etc.
  - Behavior
  - Threat risk vs. app value
- Chain Security Services
  - SSL inspection
  - Access & app protection
  - Partner ecosystem
- Execute Protection
  - Performance & scalability
  - Hybrid delivery
  - Per-app defense



A FOUNDATION FOR MORE COMPREHENSIVE SECURITY

F5 Security Messaging Hierarchy



F5 Corporate Messaging & Security Architecture Messaging

F5 App Access

F5 App Protection

Sales Plays

SSL EVERYWHERE

DDOS PROTECTION

APP PROTECTION

APP ACCESS

WEB FRAUD PROTECTION

Identifying Hybrid WAF Opportunities

4 Key Steps to Identifying a Hybrid WAF

1. Every organization needs app security

2. Identify your target persona

3. Ask target persona qualifying questions

4. Determine which WAF deployment is right

Step 1: Every Organization Needs App Security

SERIOUS VULNERABILTIES!

Government	64% of the time
Hospitality	55%
Transportation	55%
Manufacturing	51%
Other services(everything else)	53%
Healthcare	50%
Utilities	36%
Finance and Insurance	35%
Information	35%
Retail and eCommerce	29%
Education	27%

Window of exposure for at least one serious vulnerability

(WhiteHat Sec. Stats 2015)

INDUSTRY NEEDS HELP WITH!

- Critical web apps and compliance
- Apps interfacing with sensitive data
- History of downtime due to app attacks
- Cloud-based or 2 tier apps unprotected
- Finding and Patching Serious Vulnerabilities!

Step 2: Within Each Org., Identify Target Personas

EXECUTIVE LEADER

Concerned with the cost, necessity and ROI; adapting traditional business, technology, commerce, and marketing practices to a digital world.

- Managing organizational losses due to data breaches and attacks
- Maintaining compliance
- Data center consolidation

SECURITY/ NETWORK VP, DIR., ARCH.

Defines and Implements network infrastructure

- Deploys, maintains, and reports on security controls
- Investigates security incidents
- Collaborate with others to identify and define effective controls

APPLICATION OWNER

Deploys and manages the app service & roadmap and ensure the success of business/app

- Ensures services that meet key customer needs & key compliance standards
- Assess app health and ensures availability, performance and security
- Drives efforts to patch vulnerabilities

COMPLIANCE MGR

Maintain PCI regulatory compliance

- Maintains awareness of compliance risks;
- Ensures compliance
- Reports on the effectiveness of WAF solutions

Step 3: Ask Target Persona Qualifying Questions

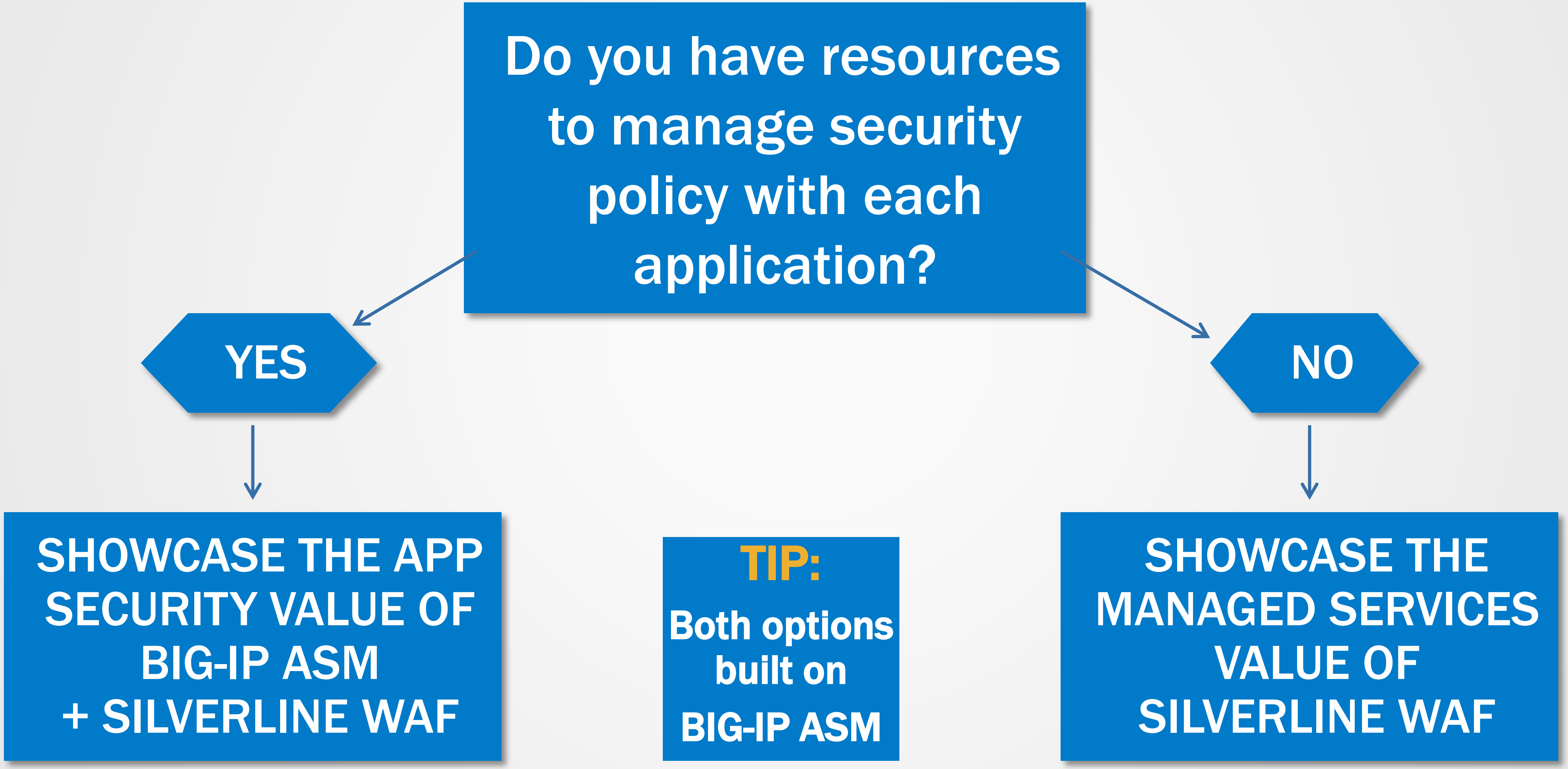
Uncover Hybrid WAF Opportunities!

- How do you protect against L7 Attacks?
- How are you complying with PCI-DSS?
- How do you reduce non-human traffic to your website?
- Do you have SaaS applications you need to deploy, or web applications you intend to migrate to the cloud? How quickly will you be able to deploy WAF policies to protect them?
- What are the implications for performance when enabling current WAF policies?

Critical Question!

- Do you have resources to manage security policy with each application?

Step 4: Determine Which WAF Deployment Is Right



Do you have resources to manage security policy with each application?

YES

NO

SHOWCASE THE APP SECURITY VALUE OF BIG-IP ASM + SILVERLINE WAF

TIP: Both options built on BIG-IP ASM

SHOWCASE THE MANAGED SERVICES VALUE OF SILVERLINE WAF

See Slide 20

See Slide 27

If Still Unclear, Consider the Following Positioning

Prospect Considerations	BIG-IP ASM	Silverline WAF	
Have resources to manage WAF	✓		Hybrid WAF Deployment
Need to maintain app blocking control	✓		
Help required from professional services	✓		
PCI compliance challenges	✓	✓	
VA/DAST part of app development/protection	✓	✓	
Must protect cloud-based apps	✓	✓	
Must protect tier 2 apps		✓	Silverline WAF Deployment
Prefer outsourcing app security		✓	
Require 3rd party policy creation with 24x7x365 support		✓	

Sell the Appropriate WAF Solution!

Selling Hybrid WAF

4 Key Steps to Selling Hybrid WAF

1 Cover key functionality in your conversation

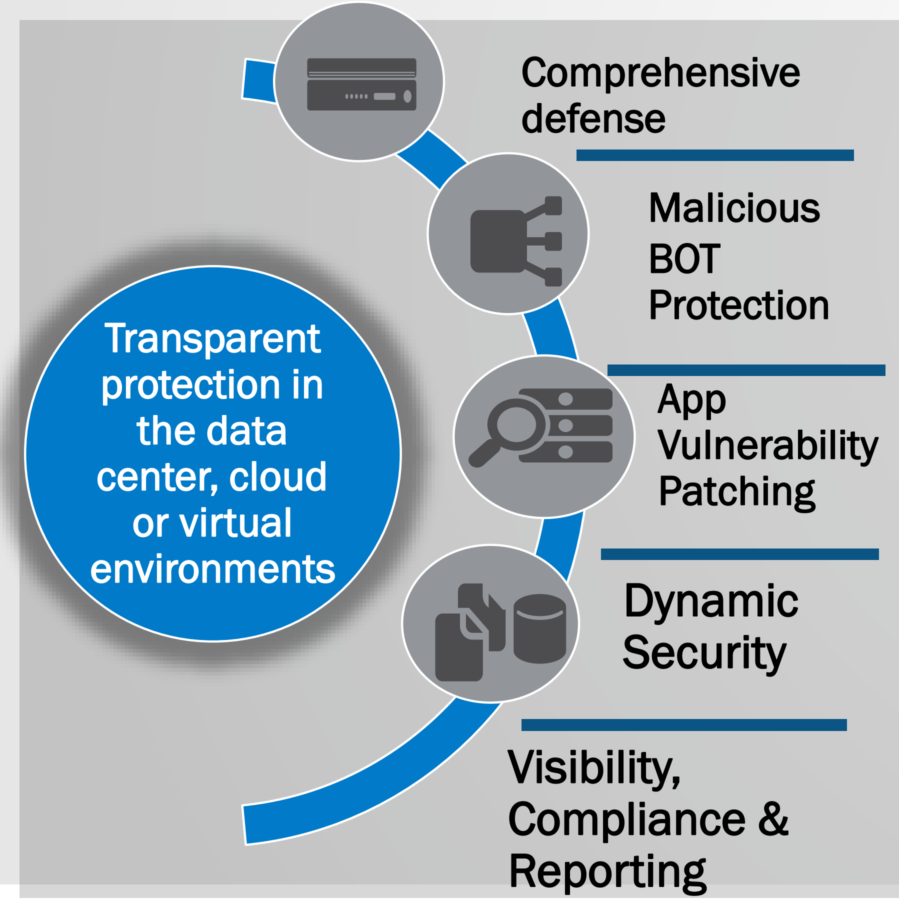
2 Highlight Hybrid WAF validations

3 Showcase the value of Hybrid WAF differentiations

4 Stress flexible deployment options and handle objections

Step 1: Cover Key Functionality In Your Conversation

PROTECTS AGAINST LAYER 7 ATTACKS WITH HIGHEST LEVEL OF GRANULARITY



Transparent protection in the data center, cloud or virtual environments

Comprehensive defense

- Delivers a full-proxy architecture with intrinsic application security
- Enables immediate defense against Layer 7 DDoS, Webscraping, and OWASP top 10

Malicious BOT Protection

- Provides a proactive defense against automated attack networks
- Identifies, blocks and enables deeper analysis of BOT attacks

App Vulnerability Patching

- Integrates with leading DAST scanners for immediate patching of vulnerabilities
- Streamlines and increases accuracy of vulnerability patching

Dynamic Security

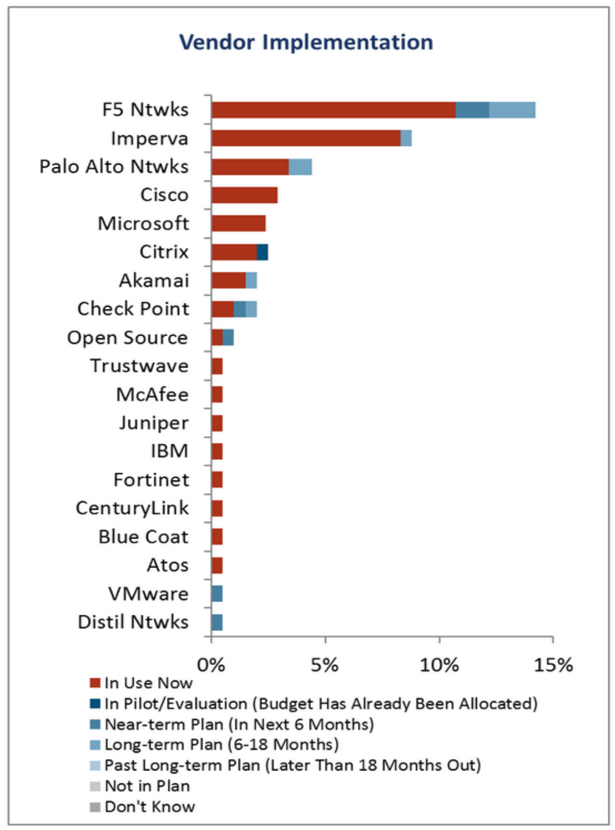
- Maintains IP Intelligence identifying bad actors and whitelisting acceptable users
- Easily correlate malicious activities with violations to identify other suspicious events

Visibility, Compliance & Reporting

- Provides quick views of events for analysis with drill downs to attack details
- Helps ensure compliance such as PCI-DSS with easy read reports and graphs

Step 2: Highlight F5 Hybrid WAF 3rd Party Validation

#1 most deployed WAF worldwide!!



#1 most effective WAF in enterprise class!!

99.89 % **Overall security effectiveness**

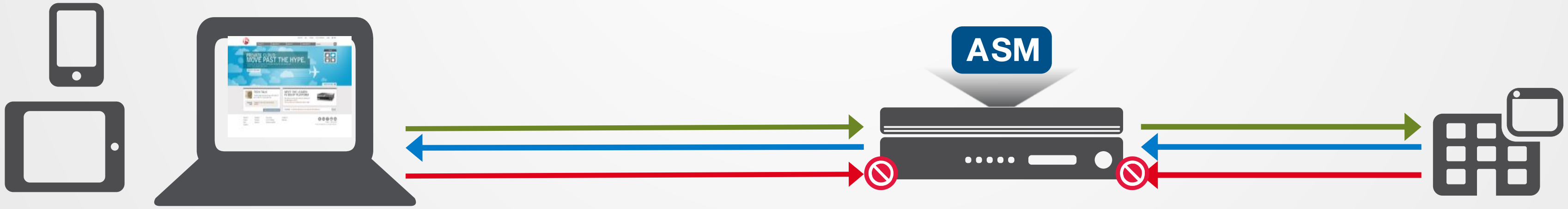
.124 % **Minimal false positives**

*451 Research reports that leadership in WAF has transitioned from Imperva to F5.

**Source: NSS Labs Web Application Firewall Product Analysis: F5 BIG-IP ASM 10200 v11.4.0;

Step 3: Showcase the Value of Hybrid WAF Differentiations

- #1 Most Effective WAF (NSS Labs)
- 2780 signatures for best protection
- Enable transparent protection from ever-changing threats
- Reduce risks from vulnerabilities with dynamic VA/ DAST integrations
- Engage unique BOT detection (rapid surfing, intervals, event sequence)
- #1 Most Deployed WAF (451 Research)
- 10 of OWASP attacks mitigated with on-box reporting
- Most programmable and extensible WAF solution available (iRules + VIPRION)
- Deploy full-proxy* or transparent full-proxy (bridge mode)

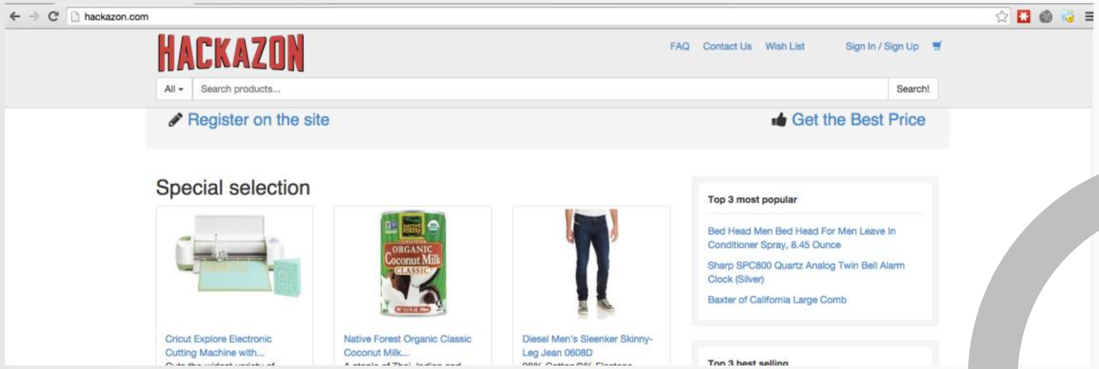


***F5 unique full-proxy WAF isolates application traffic, services, and infrastructure resources to withstand L7 attacks from client-side and server-side data leakage.**

Step 3: Highlight Dynamic One-Click Patching

Unsurpassed integrations: BIG-IP ASM and leading DAST vendors

1. Apps have vulnerabilities!


hackazon.com
HACKAZON
FAQ
Contact Us
Wish List
Sign In / Sign Up
All
Search products...
Search!
Register on the site
Get the Best Price
Special selection
Cricut Explore Electronic Cutting Machine with...
Native Forest Organic Classic Coconut Milk...
Diesel Men's Sleenker Skinny-Leg Jean 0608D
Top 3 most popular
Bed Head Men Bed Head For Men Leave In Conditioner Spray, 8.45 Ounce
Sharp SPC800 Quartz Analog Twin Bell Alarm Clock (Silver)
Baxter of California Large Comb
Top 3 best selling

- Vulnerability checking, detection and remediation
- Complete website protection

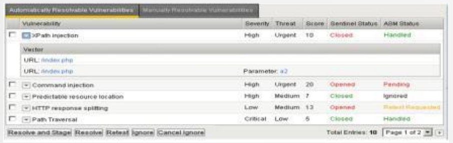
2. Recommend vulnerability assessment* (VA) scanning + virtual patching

- Finds a vulnerability
- **Virtual-patching with one-click on ASM**
- Manual patching guidance

VA/ DAST Solutions

- WhiteHat
- Qualys
- IBM
- HP

3. Fast verification and policy deployment

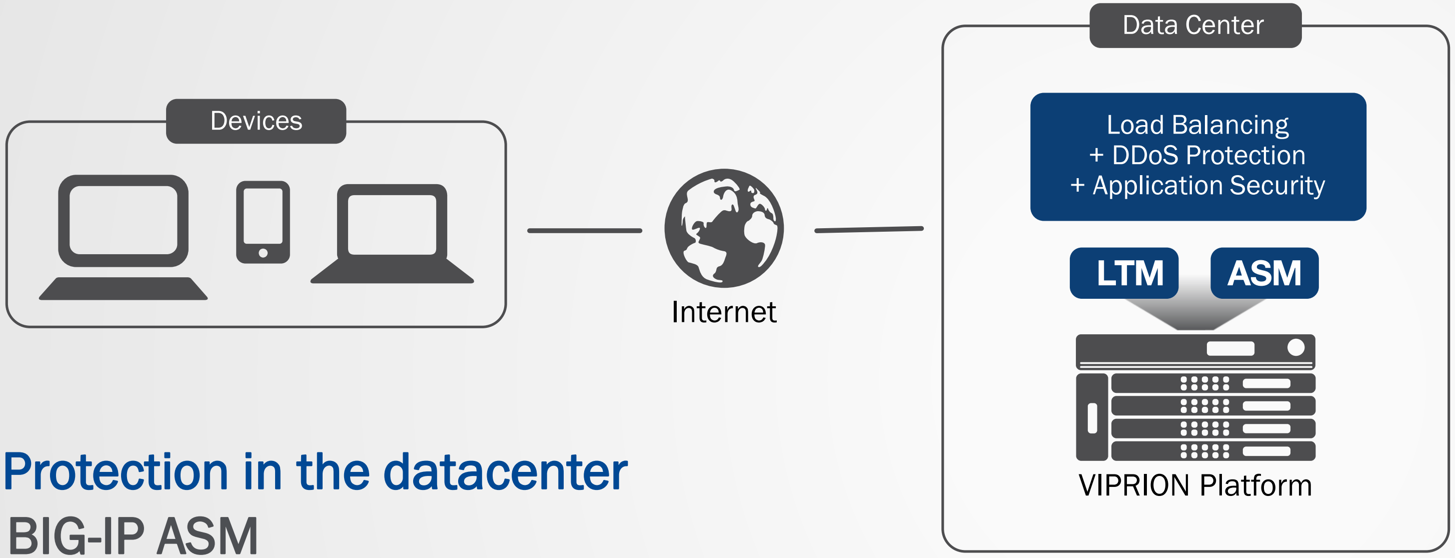

Automatically Resolvable Vulnerabilities
Manually Resolvable Vulnerabilities
Resolve and Stage
Resolve
Retest
Ignore
Cancel Ignore
Page 1 of 2

	Vulnerability	Severity	Threat	Score	Sentinel Status	ASM Status
□	XPath injection	High	Urgent	10	Closed	Handled
	Vector					
	URL: /index.php					
	URL: /index.php	Parameter: a2				
□	Command injection	High	Urgent	20	Opened	Pending
□	Predictable resource location	High	Medium	7	Closed	Ignored
□	HTTP response splitting	Low	Medium	13	Opened	Retest Requested
□	Path Traversal	Critical	Low	5	Closed	Handled

Total Entries: 10

- Verify, assess, resolve and retest in one UI
- Automatic or manual creation of policies
- Discovery and remediation in minutes
- Automatic notification of website changes*

Step 5: Stress Flexible Deployment Options



Protection in the datacenter

BIG-IP ASM

- Install on any BIG-IP platform to protect applications in the datacenter.
- Deploy as an add-on to BIG-IPs in use or run it as a standalone.

Securing applications in the cloud

ASM VE

- Activate security services close to apps that have moved to the cloud
- Accelerate development and test

F5 Silverline WAF Protection

- Recommended for fast activation of ASM protections for SMB's and enterprise-wide SAAS and tier 2 applications

Hint! Pitch Hybrid WAF in Every Deal!

Step 6: Handle Hybrid WAF Objections

Objection	Response
We already have existing protection solutions, what value does F5 add?	• F5 provides more flexible hybrid WAF protections that guard against sophisticated attacks like shell shock, poodle, and provides advanced proactive bot defense. • Hybrid WAF integrates with AFM to consolidate the datacenter, accelerate performance and protect against DDoS attacks.
We do not have familiarity with ASM and would need to develop needed skills sets	• BIG-IP ASM is an effective solution for even a novice user with step by step hints. • ASM is equipped with a set of pre-built application security policies that provide out-of-the-box protection for common apps requiring zero configuration time
Why should I choose F5 Hybrid WAF over other solutions?	• F5 Hybrid WAF delivers most comprehensive set of capabilities with highest levels of security effectiveness compared to other vendors such as Imperva. • Better price per performance than most solutions including SecureSphere and provides unsurpassed DAST support, and protection against automated Bots.

Selling Silverline WAF

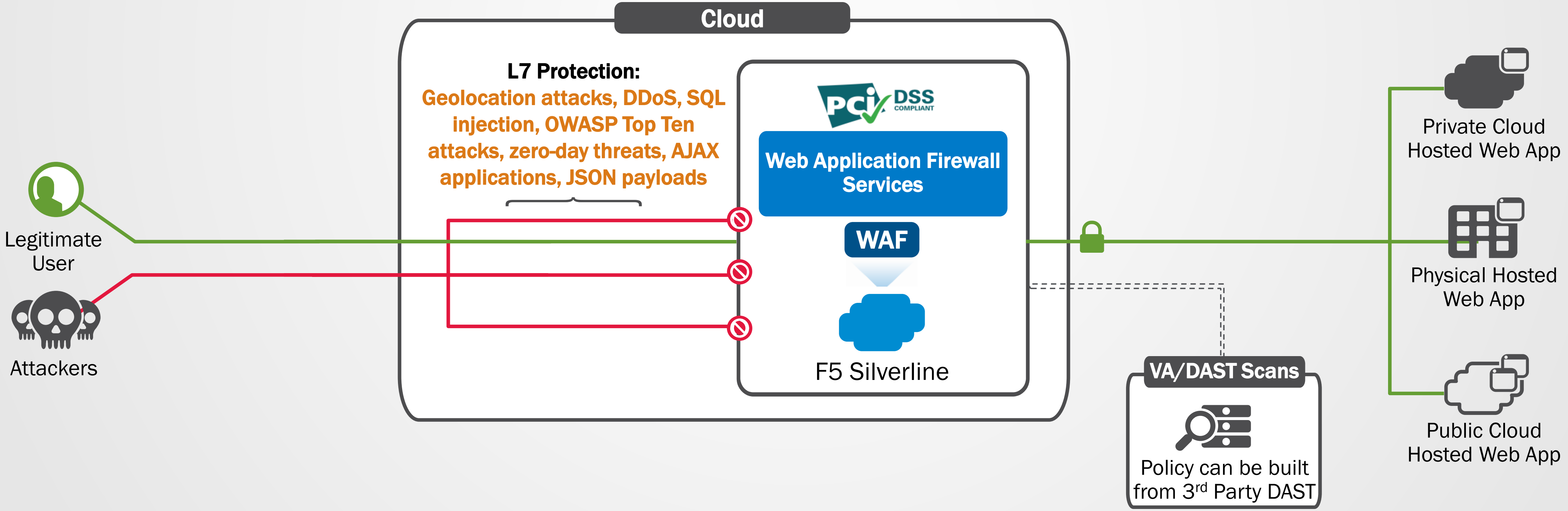
4 Key Steps to Selling Silverline WAF

1. Share key value and underscore ASM foundation
2. Position Silverline WAF appropriately
3. Emphasize the F5 SOC and key differentiators
4. Handle objections and engage Silverline sales experts

Step 1: Share Key Silverline WAF Value

Proven security effectiveness as a convenient cloud-based service

- Protect web apps and data from layer 7 attacks with F5 cloud-based WAF
- Enable compliance, such as PCI DSS
- Leverage 24x7x365 F5 SOC support for policy creation and attack management
- Outsource app security expertise


Cloud
L7 Protection:
Geolocation attacks, DDoS, SQL injection, OWASP Top Ten attacks, zero-day threats, AJAX applications, JSON payloads
PCI DSS COMPLIANT
Web Application Firewall Services
WAF
F5 Silverline
Legitimate User
Attackers
Private Cloud Hosted Web App
Physical Hosted Web App
Public Cloud Hosted Web App
VA/DAST Scans
Policy can be built from 3rd Party DAST

Step 2: Underscore ASM foundation of Silverline WAF

Runs on #1 most effective and #1 most deployed WAF

99.89% overall security effectiveness

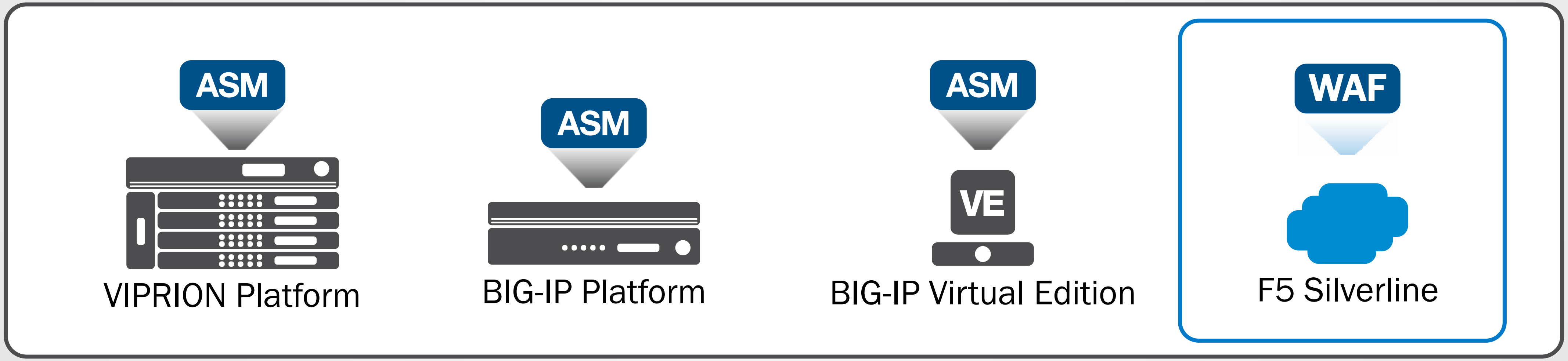
datacenters worldwide than any other WAF

on #1 ADC in the market

Deployed in more

Recognized WAF

Silverline WAF built on BIG-IP ASM



ASM

VIPRION Platform

ASM

BIG-IP Platform

ASM

VE

BIG-IP Virtual Edition

WAF

F5 Silverline

Step 3: Position Silverline WAF Appropriately

All the capabilities of BIG-IP ASM, now a managed services offering.

WHAT IT IS

- Fully managed enterprise-grade service built on BIG-IP ASM
- Service which the SOC creates, modifies, monitors and tunes all policies on behalf of the customer
- Customer portal showing violation events, proxy statistics and reports*

WHAT IT IS NOT

- Managed service for on-premises ASM within a customer's datacenter
- Self-service portal in which the customer configures their own policies (NOT Self-Service WAF)
- CDN (content distribution network)
- Pay-as-you-go, monthly, limited service

* Limited on initial release

Step 4: Focus on Two Common Use Cases

PROTECT SECONDARY WEB APPS

1. Keep BIG-IP ASM on-premises to protect primary, business-critical apps
2. Deploy Silverline Web App Firewall to protect secondary apps
   - Applications moving to the cloud
   - SaaS apps
   - Productivity apps
   - Legacy apps
   - Less frequently used apps

PROTECT ALL WEB APPS

1. Deploy Silverline WAF and protect all apps no matter where they reside
2. Drive operational and cost efficiencies
   - Customers without sufficient security staff to manage WAF policies
   - Customers building cloud datacenters
   - Need a simpler way to provide consistent WAF protections across hybrid instances

NO APP LEFT UNPROTECTED

Step 5: Emphasize The F5 Security Operations Center (SOC)

Reduce operating costs by outsourcing WAF policy management to F5 SOC experts

F5 security experts proactively monitor, and fine-tune policies to protect web applications and data from new and emerging threats.

- Expert policy setup
- Policy fine-tuning
- Proactive alert monitoring
- False positives tuning
- Detection tuning
- Whitelist / Blacklist Set up and monitoring

F5 Security Operations Center

Expert Policy Setup and Management

24/7 Availability & Support

Active Threat Monitoring

Step 6: Highlight Silverline WAF Key Differentiators

- Designed with #1 most deployed and effective WAF: BIG-IP ASM
- High level of service from F5 SOC **experts:**
  - Gain attack insights via F5 Customer Portal
  - 24x7x365 SOC support
  - Expert policy creation

- 2780 signatures for best protection
- Dynamic vulnerability protections with the ability to share VA/DAST scans
- Highly-customizable programmability
- Design iRules and iApps to protect against zero-day threats
- Future integrations with BIG-IP ASM to provide hybrid WAF services and APIs

Step 7: Handle Silverline WAF Objections

Objection	Response
Other cloud companies have 20+ POPs, you only have four. How much additional latency should I expect with F5 service?	• No other cloud competitor uses purpose-built WAF appliance such as ASM, thus no one has a greater footprint with the capabilities of Silverline WAF. • The more POPs that are introduced into a network, the longer it takes to propagate policies. This is critical when it comes to new attack vectors and zero day threats.
Other companies have bundles in performance/ CDN functionality..	• Using BIG-IP, we have many inherent performance capabilities to cache and accelerate the application, as well as industry leading SSL acceleration
The service seems to be limited in user control (self-serve).	• This was by design as the initial product was aimed towards customers who wanted the security of ASM, while reducing the complexity to manage it. • Silverline was the first to build a service that integrated with the complexity of a purposed built WAF product (ASM). More Portal updates coming soon.
I don't want to provide my SSL keys in the cloud.	• Some customers are designing a SSL DMZ where they have separate certs/keys between us and the client, and again between us and the origin.

Winning With Hybrid WAF

F5 Customer Case Studies

CARFAX®

LTM ASM APM

AFM AAM GTM VIPRION

View video on F5.com

> “The attacks happen; the attacks get blocked. If we need to change something, the interface is simple enough that we can go in and make all the adjustments in a matter of minutes—without taking anything offline.”

--Chris Thomas, Network Manager, CARFAX

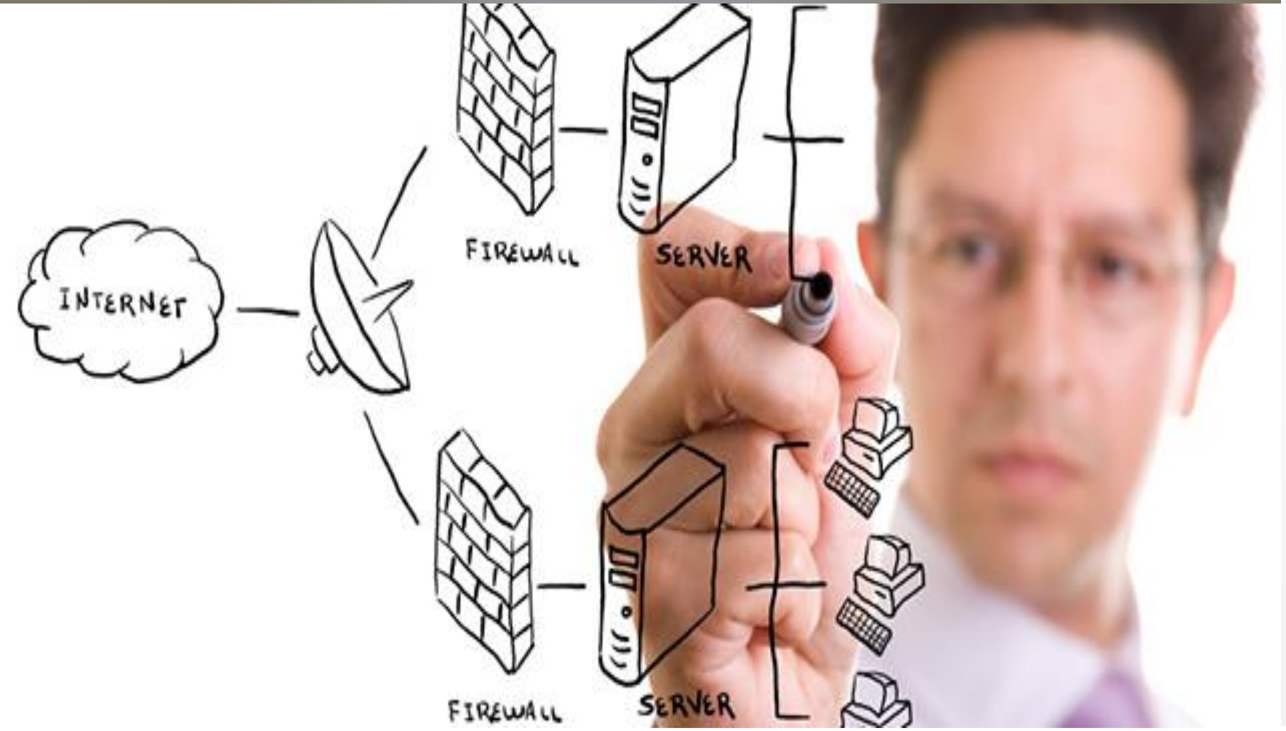
Key Benefits of F5

- Guards against data theft
- Refuse all traffic from countries where they don’t do business
- Simple UI supporting changes in minutes
- Easy to manage as part of a consolidated platform

F5 Customer Case Studies

Human Kinetics

LTM ASM



> “With the F5 solution, we’re getting far fewer false positives, so we’re allowing more legitimate traffic,” “Because F5 enables deep packet inspection, we can tell exactly what is causing an error and know how to fix it.”

– Stuart Lyons, Security Engineer at HK

Key Benefits of F5

- Reduces filtering of good traffic by minimize false positives
- Eliminates server downtime with virtual patching
- Provides more granular information , with increased flexibility and configurability
- Excellent quality of service with 24x7x365 support

How Customers Buy F5

As they deploy F5 to more of their application portfolio across the traditional datacenter and private & public cloud environments, F5 offers customers a variety of programs optimized for their hybrid cloud strategies and right-sized for CAPEX and OPEX budgets.

Flexible Options To Meet Customers Where They Are Going

1. Platforms: Create great customer value with blended platform options

2. Licensing: Choose flexible options across perpetual licensing, subscription models and on-demand pricing

3. Services: Select a variety of F5 services and support options to help customers succeed

4. Sizing: Build out the right requirements for ASM and Silverline WAF quotes

Platforms: Create Great Customer Value

F5 Platforms

Virtual

F5 software

Provide flexible deployment options for virtual environments and the cloud with Virtual Edition

Virtual Edition is best for:

- Accelerated deployment
- Maximizing data center efficiency
- Private and public cloud deployments
- Application or tenant-based pods
- Keeping security close to the app
- Lab, test, and QA deployments

Physical

F5 hardware

High-performance with specialized and dedicated hardware

Physical Hardware is best for:

- Fastest performance
- Highest scale
- SSL offload, compression, and DoS mitigation
- An all F5 solution: integrated HW+SW
- Edge and front door services
- Purpose-built isolation for application delivery workloads

Hybrid

Physical + virtual = hybrid ADC infrastructure

Ultimate flexibility and performance

Hybrid is best for:

- Transitioning from physical to virtual and private data center to cloud
- Cloud bursting
- Splitting large workloads
- Tiered levels of service

*Note: 2000 Series appliances is not offered with Better or Best bundles

Licensing: Choose Flexible Software Options

Cloud options tailored to customer needs for greater flexibility and choice

Volume of F5-backed Apps →

Cloud Licensing Program (CLP)	Bring Your Own License (BYOL)	Volume Licensing Subscription (VLS)
On-demand Utility pricing with highest flexibility; pay-as-you-go or annual subscription.	Perpetual VE License which customer owns and can move across private and public clouds.	Subscription discounts for 100+ applications; 1 or 3-year terms, up to 78% discount. Includes premium support services.
Public cloud	Public, private, and hybrid	Public, private and hybrid
Best for deployment flexibility; on-demand consumption	**Best for** few production workloads or existing licenses	**Best for** large scale workload production; F5 for every app.
OPEX	CAPEX	OPEX
via F5 Ready Cloud Provider	via F5 or channel partner	

← Price/License

$$$	$$	$

Licensing: Find an F5 Ready Public Cloud Provider

Verified by F5 for greater cloud confidence

F5-verified

BIG-IP products verified by F5 for compatibility in F5 Ready clouds.

Global-reaching

F5-verified providers span Americas, EMEA, and APAC for broad reach and selection.

Flexible

Variety of purchase options: BYOL, on-demand Utility billing, Volume Licensing Subscription.

amazon webservices™

BT

vmware® READY vCLOUD® AIR™

Microsoft Azure

DATACOM

CISCO™

bluelock®

Skytap

SINGLEHOP® | HOSTING

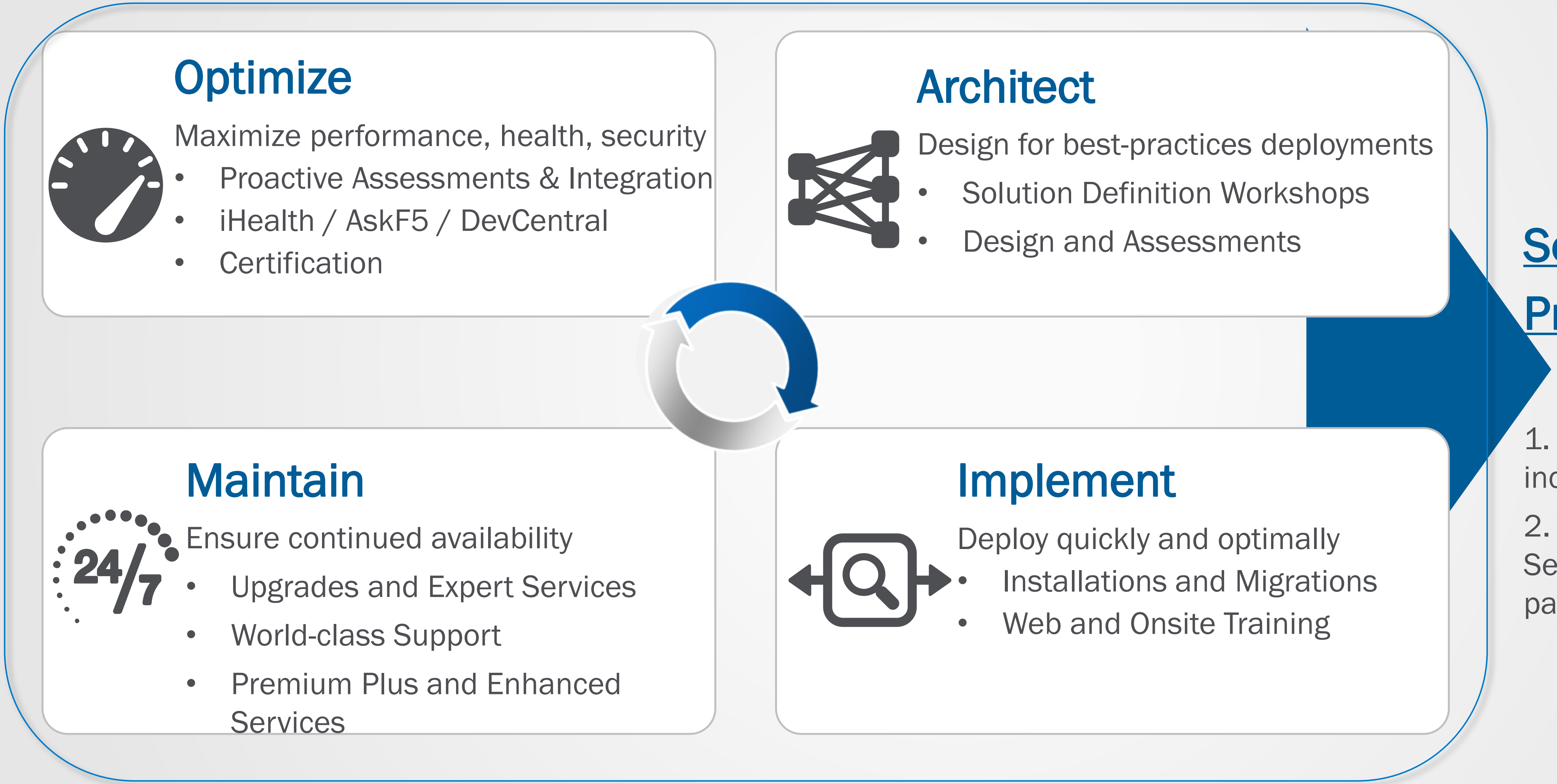
dimension data

rackspace®

Note: F5 adds new partners on a regular cadence, check f5.com/f5ready for the most up-to-date list

Services: Select A Variety of Service and Support Options

Drive Greater ROI With Customers Throughout The Solution Lifecycle



Optimize

Maximize performance, health, security

- Proactive Assessments & Integration
- iHealth / AskF5 / DevCentral
- Certification

Architect

Design for best-practices deployments

- Solution Definition Workshops
- Design and Assessments

Maintain

Ensure continued availability

- Upgrades and Expert Services
- World-class Support
- Premium Plus and Enhanced Services

Implement

Deploy quickly and optimally

- Installations and Migrations
- Web and Onsite Training

Sell App Security Pro. Services:

1. ASM deployment service including policy creation
2. VA/DAST Mitigation Service for virtual one-click patching

Services: Optimized For Customer Initiatives

End-to-end Global Services and Support Options

	Traditional ADC	Security	Cloud
Architect Design for best practices	Solution Definition Workshop		
Implement Quick and optimal	Deployment & Migration Services		
	Training and Certification		
Maintain Backed by F5 Support	Maintenance Agreements		
	Premium Plus Support		
Optimize Maximize performance, health, security	Customization & Scripting		
	iHealth Diagnostics & Self-help Tools		

Services: Flexible Options

Packaged, Custom & Hourly

Flexible F5 Purchase Options

Packaged

License: Fixed Price

Scoped to meet popular customer solutions.

Focus: Customer and technology trends. Carefully aligned with F5 pricing bundles and popular customer solutions.

Custom

License: Custom

Scoped to meet your specific business and solution needs. Flexible procurement options.

Focus: Complex or unique solutions, or where a customer can leverage our deep skills.

Hourly

License: Hourly

Small-scale services for ad-hoc customization and scripting

Focus: Extended application verification, complex monitors, iRules scripting, iControl API, and other automated tasks.

Partner Services

f5 Guardian Unity Partner

F5 UNITY Gold or Platinum Partners

Dedicated Professional Services staff backed by F5 certifications

Sizing: Build Out The Right Requirements for Quotes

Sales is often asked how to size ASM for an opportunity?

The short answer is: You need to work with your Channel SE.

Key things to discuss with the customer:

- Transactions per second TPS?
- HTTP RPS average request size?
- Do they have a team that is focused on application security? and patching application holes?
- Do they want to set & forget to solve a compliance check-box?
- Do they have a DAST (Whitehat) that will drive policy maintenance?
- Is ASM going to be colocated with something else? (APM, AFM, AAM, LTM)
- What's going to consume the ASM logs, because we don't want that on-box?

BIG-IP ASM SKU Examples

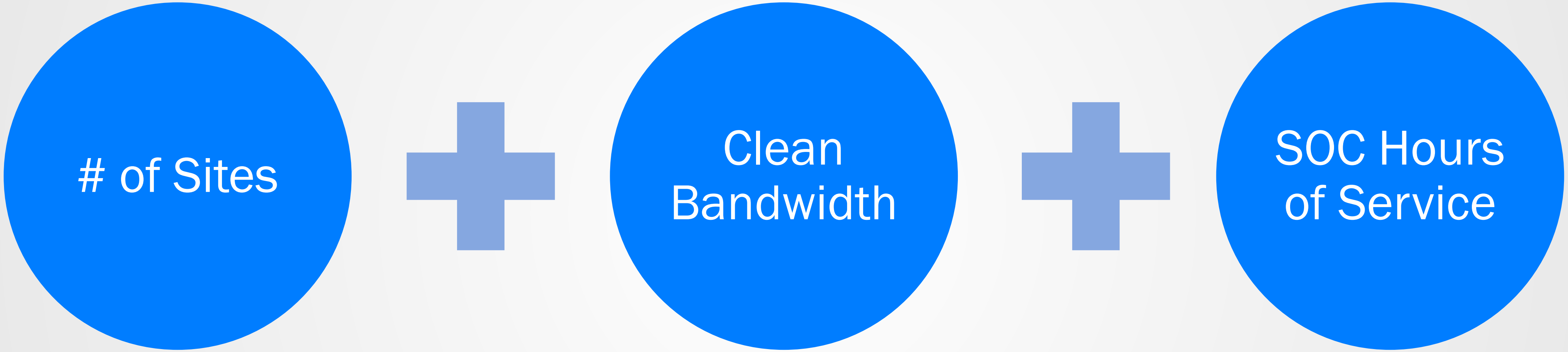
SKU	Description
F5-BIG-ASM-4200V	Application Security Manager standalone (16 GB Memory, Max SSL, Max Compression)
F5-ADD-BIG-ASM-4000	BIG-IP Application Security Manager Add-on Software Module for 4200v/4000s
F5-BIG-BT-4200V	BIG-IP 4200v Best Bundle (16 GB Memory, Max SSL, Max Compression)

BIG-IP ASM VE and Cloud Examples

SKU	Description
F5-BIG-ASM-VE-1G-V13	BIG-IP Virtual Edition Application Security Manager 1 Gbps (v11.4.1 - v15.x)
F5-BIG-VE-BT-1G-V13	BIG-IP Virtual Edition Best Bundle 1 Gbps (v11.4.1 - v15.x)
F5-BIG-VLSBTMXG1001Y	BIG-IP Virtual Edition Best Bundle Max Volume Licensing Subscription (100 Instances, 1 Year)

Sizing: Build Out The Right Requirements for Quotes

- Cost of service is determined by:



# of Sites

+

Clean Bandwidth

+

SOC Hours of Service

- Upgrades are available for additional sites, bandwidth, and extended support.

Contact your F5 Channel Account Manager for more information

Sizing: Build Out The Right Requirements for Quotes

Silverline Web Application Firewall Subscription

1YR SKU	3YR SKU	# of Sites	Bandwidth (95th percentile)
F5-FAS-WAF-5S-50M-1Y	F5-FAS-WAF-5S-50M-3Y	5	50 Mbps/month
F5-FAS-WAF-10S100M1Y	F5-FAS-WAF-10S100M3Y	10	100 Mpbs/month
F5-FAS-WAF-50S500M1Y	F5-FAS-WAF-50S500M3Y	50	500 Mpbs/month
F5-FAS-WAF-100S-2G1Y	F5-FAS-WAF-100S-2G3Y	100	2 Gbps/month
F5-FAS-WAF-200S-2G1Y	F5-FAS-WAF-200S-2G3Y	200	2 Gbps/month

+

Recommended SOC Service SKUs based on Sites/Bandwidth

Required SOC Services

Hours of Service	SKU
20 hrs Per SKU	F5-FAS-SOCS-20H-1Y
40 hrs Per SKU	F5-FAS-SOCS-40H-1Y
60 hrs Per SKU	F5-FAS-SOCS-60H-1Y
80 hrs Per SKU	F5-FAS-SOCS-80H-1Y
100 hrs Per SKU	F5-FAS-SOCS-100H-1Y
1hr for extended work	F5-UTL-FAS-SOCS-1H

Upgrades

Additional Bandwidth

1YR SKU	3YR SKU	Additional Bandwidth
F5-FAS-WAF-ADD-50M1Y	F5-FAS-WAF-ADD-50M3Y	Add 50 Mbps/month
F5-FAS-WAF-ADD100M1Y	F5-FAS-WAF-ADD100M3Y	Add 100 Mpbs/month
F5-FAS-WAF-ADD500M1Y	F5-FAS-WAF-ADD500M3Y	Add 500 Mpbs/month
F5-FAS-WAF-ADD-1G-1Y	F5-FAS-WAF-ADD-1G-3Y	Add 1 Gbps/month

Additional Sites

1YR SKU	3YR SKU	Additional Sites
F5-FAS-WAF-ADD-5S-1Y	F5-FAS-WAF-ADD-5S-3Y	Add 5 Sites
F5-FAS-WAF-ADD-10S1Y	F5-FAS-WAF-ADD-10S3Y	Add 10 Sites
F5-FAS-WAF-ADD-50S1Y	F5-FAS-WAF-ADD-50S3Y	Add 50 Sites
F5-FAS-WAF-ADD100S1Y	F5-FAS-WAF-ADD100S3Y	Add 100 Sites

Bandwidth is totaled across all sites, NOT per site. SOC hours expire after 1 year.

Call to Action

Review all App. Security use cases, and opportunities leveraging available resources as you increase F5 BIG-IP ASM and Silverline WAF sales

Identify current portfolio and new prospects that need or find value in cloud-based application services

Enable prospect education on F5 hybrid WAF use cases, benefits, services, and sales tools

Deliver growth by recommending F5 Web App Firewall services for all hybrid environments

YOUR MISSION: SELL HYBRID WAF!

NO APP LEFT UNPROTECTED

BIG-IP Platform

F5 Silverline

Solutions for an application world.