Selling Web Application Firewall Solutions

Jonathan George
Sr. Product Marketing Manager
## Agenda

### WAF SALES PLAY

<table>
<thead>
<tr>
<th>Sales Play Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market and Customer Challenges</td>
</tr>
<tr>
<td>Identify Hybrid WAF Opportunities</td>
</tr>
<tr>
<td>Selling Hybrid WAF (BIG-IP ASM and Silverline WAF)</td>
</tr>
<tr>
<td>Selling Silverline WAF</td>
</tr>
<tr>
<td>Winning with Hybrid WAF</td>
</tr>
</tbody>
</table>
Web Application Firewall Sales Play

Learn more about showing prospects the value of F5 Web Application Firewall capabilities. Share BIG-IP Application Security Manager (ASM) the #1 most deployed and #1 most effective WAF in class to solve critical app security needs on prem. and across hybrid cloud. For tier 2 apps on prem. and cloud-based applications, share Silverline Web Application Firewall designed on BIG-IP ASM for complete app protection managed by a 24x7x365 SOC team for prospects without IT resources. Share the combined F5 Hybrid WAF solution offerings to cover all apps enabling no app left unprotected.

View the Channel Playbook
View the Sales Play Battlecard
View the Sales Play Customer Presentation
WAF Training

This playbook assumes a basic understanding of BIG-IP Application Security Manager (ASM) and Silverline Web Application Firewall 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/](https://university.f5.com/)
- Follow us on f5.com: [Application Security Manager](https://university.f5.com/)
- Manuals and Release Notes on f5.com

**Silverline Web Application Firewall education**
Product information
- Follow us on f5.com: [Silverline WAF](https://university.f5.com/)
- Onboarding Tech. Notes on f5.com
Understand 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
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 60% of public web apps will use WAFs delivered as a cloud service or internet-hosted virtual appliance by 2020

WAF Total Addressable Market

- Technavio, 2015
- Infonetics, Q4CY2013
- IDC, 2013
- Gartner WAF MQ 2015, F5

F5: Recognized as Leading Challenger in Growing Market
Important Trends in Threat Vectors
Important Trends in Threat Vectors

- **20%** of IT pros are confident users avoid phishing.
  
  **86%** of websites have at least 1 serious vulnerability.
  
  **23 min** average time to be hit by a critical exploit.
  
  **56** average number of vulnerabilities per website.
  
  **56%** of security professionals employ WAF.

**WhiteHat Security Statistics Report 2015**

- **85,000** malicious IPS launched everyday.
  
  **2.3M** bots actively attacking.

**Threat Brief Report, Webroot, May 2015**

**Symantec Internet Security Report 2014**

© 2016 F5 Networks
Application Threats Increase Challenges and Complexity
Application Threats Increase Challenges and Complexity

How can I protect cloud and SaaS applications quickly?

Where can I find WAF policy experts?

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

How can I maintain compliance across hybrid environments?

How can I scale protection without upfront IT investments?

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!

<table>
<thead>
<tr>
<th></th>
<th>Traditional Network Perimeter</th>
<th>Per-App/Per-User Perimeter</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL-visible</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Location-independent</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Session-based</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Continuous trust verification</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Strategic control points</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>App availability</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

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

WEB APPLICATION FIREWALL

IDENTITY FEDERATION

WEB FRAUD PROTECTION

Rethink Security Architectures with App Perimeter
F5 Security Messaging Hierarchy

F5 Corporate Messaging & Security Architecture Messaging

F5 App Access

F5 App Protection

Sales Plays

SSL EVERYWHERE

DDOS PROTECTION

WEB APPLICATION FIREWALL

IDENTITY FEDERATION

WEB FRAUD PROTECTION

Rethink Security Architectures with App Perimeter
Identifying Hybrid WAF Opportunities
4 Key Steps to Identifying a Hybrid WAF

1. Every organization needs app security
2. Identify target decision makers
3. Ask target persona qualifying questions
4. Determine which WAF deployment is right
Step 1: Every Organization Needs App Security

### Serious Vulnerabilities

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>64%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>55%</td>
</tr>
<tr>
<td>Transportation</td>
<td>55%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>51%</td>
</tr>
<tr>
<td>Other services</td>
<td>53% (everything else)</td>
</tr>
<tr>
<td>Healthcare</td>
<td>50%</td>
</tr>
<tr>
<td>Utilities</td>
<td>36%</td>
</tr>
<tr>
<td>Finance and Ins.</td>
<td>35%</td>
</tr>
<tr>
<td>Information</td>
<td>35%</td>
</tr>
<tr>
<td>Retail &amp; eCommerce</td>
<td>29%</td>
</tr>
<tr>
<td>Education</td>
<td>27%</td>
</tr>
</tbody>
</table>

### 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!

Window of exposure for at least one serious vulnerability (WhiteHat Sec. Stats 2015)
<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EXECUTIVE LEADER</strong></td>
<td>Concerned with the cost, necessity and ROI; adapting traditional business, technology, commerce, and marketing practices to a digital world</td>
</tr>
<tr>
<td><strong>SECURITY/NETWORK VP, DIR., ARCH.</strong></td>
<td>Defines and implements network infrastructure</td>
</tr>
<tr>
<td><strong>APPLICATION OWNER</strong></td>
<td>Deploys and manages the app service and roadmap, and ensures the success of business/app</td>
</tr>
<tr>
<td><strong>COMPLIANCE MGR</strong></td>
<td>Maintains PCI regulatory compliance</td>
</tr>
</tbody>
</table>

- Managing organizational losses due to data breaches and attacks
- Maintaining compliance
- Data center consolidation
- Deploys, maintains, and reports on security controls
- Investigates security incidents
- Collaborates with others to identify and define effective controls
- Ensures services that meet key customer needs and key compliance standards
- Assesses app health and ensures availability, performance, and security
- Drives efforts to patch vulnerabilities
- 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

Showcase the app security value of BIG-IP ASM and Silverline WAF

See Slide 22

NO

TIP: Both options built on BIG-IP ASM

Showcase the managed services value of Silverline WAF

See Slide 31
Step 4: If Still Unclear, Consider the Following Positioning

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

Hybrid WAF Deployment

Silverline WAF Deployment

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
### PROTECTS AGAINST LAYER 7 ATTACKS WITH HIGHEST LEVEL OF GRANULARITY

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Comprehensive defense** | - Delivers a full-proxy architecture with intrinsic application security  
- Enables immediate defense against layer 7 DDoS, web scraping, 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, and 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 Third-Party Validation

#1 MOST DEPLOYED WAF WORLDWIDE

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

#1 MOST EFFECTIVE WAF IN ENTERPRISE CLASS

99.89%
Overall security effectiveness

124%
Minimal false positives

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

Learn More: https://hive.f5.com/message/72206#72206
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 effective 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’S 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: Only Vendor with Dynamic One-Click Patching

Unsurpassed integrations: BIG-IP ASM and leading DAST vendors

1. Apps have vulnerabilities!

2. Recommend vulnerability assessment (VA) scanning + virtual patching
   - Virtual-patching with one-click on BIG-IP ASM
   - Manual patching guidance

3. Fast verification and policy deployment
   - 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 4: Stress Flexible Deployment Options

**Protection in the data center**

**BIG-IP ASM**
- Install on any BIG-IP platform to protect applications in the data center.
- Deploy as an add-on to BIG-IP products in use or run it as a standalone.

**Securing applications in the cloud**

**BIG-IP 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 SMBs and enterprise-wide SAAS and tier 2 applications.

**HINT:** RECOMMEND HYBRID WAF IN EVERY DEAL!
Selling Silverline
Web Application Firewall
4 Key Steps to Selling Silverline WAF

1. Share key value and underscore BIG-IP 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
- Built on #1 most effective WAF (99.89%) in class

- Leverage 24x7x365 F5 SOC support for policy creation and attack management
- Outsource app security expertise
- Built on #1 deployed WAF

L7 Protection:
- Geolocation attacks, DDoS, SQL injection, OWASP Top Ten attacks, zero-day threats, AJAX applications, JSON payloads

Cloud

Web Application Firewall Services

F5 Silverline

VA/DAST
Policy can be built from 3rd Party DAST
Step 2: Position Silverline WAF Appropriately

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

<table>
<thead>
<tr>
<th>WHAT IT IS</th>
<th>WHAT IT IS NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Fully managed, enterprise-grade service built on BIG-IP ASM</td>
<td>• Managed service for on-premises BIG-IP ASM within a customer’s data center</td>
</tr>
<tr>
<td>• Service in which the SOC creates, modifies, monitors, and tunes all policies on behalf of the customer</td>
<td>• Self-service portal in which the customer configures their own policies (NOT self-service WAF)</td>
</tr>
<tr>
<td>• Customer portal showing violation events, proxy statistics and reports*</td>
<td>• CDN (content distribution network)</td>
</tr>
<tr>
<td></td>
<td>• Pay-as-you-go, monthly, limited service</td>
</tr>
</tbody>
</table>

* Limited on initial release
Step 2: Focus on Two Common Use Cases

<table>
<thead>
<tr>
<th>PROTECT SECONDARY WEB APPS</th>
<th>PROTECT ALL WEB APPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Keep BIG-IP ASM on-premises to protect primary, business-critical apps</td>
<td>1. Deploy Silverline WAF and protect all apps <em>no matter where they reside</em></td>
</tr>
<tr>
<td>2. Deploy Silverline Web App Firewall to protect secondary apps</td>
<td>2. Drive operational and cost efficiencies</td>
</tr>
<tr>
<td>• Applications moving to the cloud</td>
<td>• Customers without sufficient security staff to manage WAF policies</td>
</tr>
<tr>
<td>• SaaS apps</td>
<td>• Customers building cloud data centers</td>
</tr>
<tr>
<td>• Productivity apps</td>
<td>• Need a simpler way to provide consistent WAF protections across hybrid instances</td>
</tr>
<tr>
<td>• Legacy apps</td>
<td>• Less frequently used apps</td>
</tr>
<tr>
<td>• Less frequently used apps</td>
<td></td>
</tr>
</tbody>
</table>
Step 3: 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 customer portal visibility
Step 3: Highlight Silverline WAF Key Differentiators

- Designed with #1 most deployed and effective WAF in class: 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
Winning with Hybrid WAF
"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

View video on F5.com
“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
Platforms: Create Great Customer Value

F5 Platforms

Virtual

F5 software
Provide flexible deployment options for virtual environments and the cloud with virtual editions

Virtual editions are 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
Virtual Editions: Find an F5-Ready Public Cloud Provider

Verified by F5 for greater cloud confidence

**F5-Verified**
BIG-IP VE 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.

Note: F5 adds new partners on a regular cadence, check f5.com/f5ready for the most up-to-date list
Drive Greater ROI with Services—2 Choices
Driving customer satisfaction throughout the solution lifecycle

DEVELOP AND RESELL YOUR SERVICES
Maximize performance, health, security
- Product Training [F5 University](#)
- F5 UNITY Gold or Platinum Partner Status
- F5 Certified Engineer(s)
- Proactive Assessments and Integration Services
- Utilizing iHealth/AskF5/DevCentral

RESELL F5 PROFESSIONAL SERVICES
Recommended practices design deployment utilizing:
- Solution Definition Workshops (SDW)
- Projection Definition Workshop (PDW)
- Design and Implementation Services
- Migration and Upgrade Services

Americas: [consultingsales@f5.com](mailto:consultingsales@f5.com)
Make More Money Selling F5 Hybrid WAF Products!

What’s in it for you?
• Expand your business and sell WAF products to protect all web apps
• Increase deal size of existing security solutions with F5 hybrid WAF (BIG-IP ASM and Silverline Web Application Firewall)
• Set the stage for future solution offerings tied to the broader F5 security portfolio

Channel Program: Vault Security Program
• Earn up to up to $20,000 for each qualified Vault Security opportunity
• Earn a 2x accelerator when you sell Silverline WAF with qualifying VAULT SKUs
• Sell Better or Best Virtual Edition Volume License Subscription (VLS)
• Stack your incentives for the highest payout

Landing Page on Partner Central
Call to Action

**Review** all app. security use cases and opportunities leveraging Partner Central resources and your CAM as you increase BIG-IP ASM and Silverline Web Application Firewall 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.
Give Feedback – Get Points!

- Add class to your personal schedule.
- Survey will pop up in Mobile App.
- Answer the multiple choice.
- Submit your question to complete.
- Receive 5 points!
Important Trends in Threat Vectors

INTERNET OF THINGS
Important Trends in Threat Vectors

INTERNET OF THINGS

100s

EMERGING DEVICES AND APPLICATIONS
Application Attacks Hurt Your Business
Evolving Security Threats

Cyber Security Intelligence Index
Application Attacks Hurt Your Business

Evolving Security Threats

$7.7M
Average cost of cyber crime per company\(^1\)

99
Successful attacks per year per company\(^1\)

81M
Monitored cyber attacks Worldwide\(^2\)

Source 1: Ponemon Institute, 2015 Cost of Cyber Crime Study, 2 IBM Security Services, 2015 Cyber Security Intelligence Index
Application Attacks Hurt Your Business

Evolving Security Threats

- **$7.7M**: Average cost of cyber crime per company
- **99**: Successful attacks per year per company
- **81M**: Monitored cyber attacks Worldwide

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, 2015 Cost of Cyber Crime Study
Source 2: IBM Security Services, 2015 Cyber Security Intelligence Index
Step 1: Underscore ASM foundation of Silverline WAF

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

99.89% overall security effectiveness

Deployed in more datacenters worldwide than any other WAF

Recognized WAF on #1 ADC in the market

Silverline WAF built on BIG-IP ASM
## Step 4: Handle Hybrid WAF Objections

<table>
<thead>
<tr>
<th>Objection</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>We already have existing protection solutions. What value does F5 add?</td>
<td>• F5 provides more flexible hybrid WAF protections that guard against sophisticated attacks like shellshock and poodle, and provides advanced proactive bot defense.</td>
</tr>
<tr>
<td></td>
<td>• Hybrid WAF products integrate with BIG-IP AFM to consolidate the data center, accelerate performance, and protect against DDoS attacks.</td>
</tr>
<tr>
<td>We do not have familiarity with ASM and would need to develop needed skills sets</td>
<td>• BIG-IP ASM is an effective solution for even a novice user with step by step hints.</td>
</tr>
<tr>
<td></td>
<td>• BIG-IP 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.</td>
</tr>
<tr>
<td>Why should I choose F5 hybrid WAF products over other solutions?</td>
<td>• F5 hybrid WAF products deliver most comprehensive set of capabilities with highest levels of security effectiveness compared to other vendors such as Imperva.</td>
</tr>
<tr>
<td></td>
<td>• Better price per performance than most solutions including SecureSphere and provides unsurpassed DAST support and protection against automated Bots.</td>
</tr>
<tr>
<td>How do I successfully compete as a challenger in Gartner WAF Magic Quadrant?</td>
<td>• BIG-IP ASM is a leading contender in WAF market and has a clear advantage with on-premises deployment and completeness of solution are the key drivers.</td>
</tr>
<tr>
<td></td>
<td>• To compete successfully, lead with advanced DDoS protections, best bot defense, securing against vulnerability exploits and protect against OWASP top 10.</td>
</tr>
</tbody>
</table>
## Step 4: Handle Silverline WAF Objections

<table>
<thead>
<tr>
<th>Objection</th>
<th>Response</th>
</tr>
</thead>
</table>
| Other cloud companies have 20+ POPs, you only have four. How much additional latency should I expect with your service? | • No other cloud competitor uses purpose-built WAF appliance such as BIG-IP ASM, thus no one has a greater footprint with the capabilities of Silverline Web Application Firewall.  
• 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 the BIG-IP platform, 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 BIG-IP ASM, while reducing the complexity to manage it.  
  • Silverline was the first to build a service that integrated with the complexity of a purpose-built WAF product (BIG-ASM). More portal updates coming soon.  
  • 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. |
| I don’t want to provide my SSL keys in the cloud.                         |                                                                                                                                                                                                          |
### Services: Optimized for Customer Initiatives

End-to-end Global Services and Support Options

<table>
<thead>
<tr>
<th></th>
<th>Traditional ADC</th>
<th>Security</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Architect</strong></td>
<td>Design for best practices</td>
<td>Solution Definition Workshop</td>
<td></td>
</tr>
<tr>
<td><strong>Implement</strong></td>
<td>Quick and optimal</td>
<td>Deployment &amp; Migration Services</td>
<td>Training and Certification</td>
</tr>
<tr>
<td><strong>Maintain</strong></td>
<td>Backed by F5 Support</td>
<td>Maintenance Agreements</td>
<td>Premium Plus Support</td>
</tr>
<tr>
<td><strong>Optimize</strong></td>
<td>Maximize performance, health, security</td>
<td>Customization &amp; Scripting</td>
<td>iHealth Diagnostics &amp; Self-help Tools</td>
</tr>
</tbody>
</table>
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. BIG-IP ASM deployment service including policy creation
2. VA/DAST mitigation service for virtual one-click patching
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
24/7
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. BIG-IP ASM deployment service including policy creation
2. VA/DAST mitigation service for virtual one-click patching

Drive Greater ROI with Customers Throughout the Solution Lifecycle
## Services—Driving Customer Satisfaction & Your Bottom Line

<table>
<thead>
<tr>
<th>Architect</th>
<th>Implement</th>
<th>Maintain</th>
<th>Optimize</th>
</tr>
</thead>
</table>
| - Detailed architectural planning delivered by F5 and partner | - BIG-IP Application Security Manager (on premises)  
  - BIG-IP ASM deployment service including policy creation  
  - VA/DAST mitigation service for virtual one-click patching | - F5 maintenance packages  
  - Standard @ 12%  
  - Premium @ 17%  
  - Leverage F5’s self-solve capabilities to support and optimize our customers solutions  
  - [https://f5.com/support/self-solve](https://f5.com/support/self-solve) From here partners (& customers) have access to all the self-solve content and information |
| - Provides our shared customers a detailed view of F5 solutions to a strategic business need | | - BIG-IP LTM upgrade assessment service  
  - BIG-IP ASM upgrade assessment service | |
| - F5-CST-PKG-SDW: $15,000 | | | |

© 2016 F5 Networks
Sales is often asked how to size BIG-IP ASM for an opportunity. The short answer is: **You need to work with your Regional Security SME (Channel SE).**

Key things to discuss with the customer that will help your SME:

- 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 and forget to solve a compliance check box?

If you have an opportunity with a customer, please fill out answers to above questions to expedite the sales lifecycle.

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5-BIG-ASM-4200V</td>
<td>Application Security Manager standalone (16 GB Memory, Max SSL, Max Compression)</td>
<td>F5-BIG-ASM-VE-1G-V13</td>
<td>BIG-IP Virtual Edition Application Security Manager 1 Gbps (v11.4.1 - v15.x)</td>
</tr>
<tr>
<td>F5-ADD-BIG-ASM-4000</td>
<td>BIG-IP Application Security Manager Add-On Software Module for 4200v/4000s</td>
<td>F5-BIG-VE-BT-1G-V13</td>
<td>BIG-IP Virtual Edition Best Bundle 1 Gbps (v11.4.1 - v15.x)</td>
</tr>
<tr>
<td>F5-BIG-BT-4200V</td>
<td>BIG-IP 4200v Best Bundle (16 GB Memory, Max SSL, Max Compression)</td>
<td>F5-BIG-VLSBTMXG1001Y</td>
<td>BIG-IP virtual edition Best Bundle Max Volume Licensing Subscription (100 Instances, 1 Year)</td>
</tr>
</tbody>
</table>
Sizing: Build Out the Right Requirements for Quotes

• Work with Channel Sales to scope the opportunity and choose the right SKUs for your customer.

• 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

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

### Required SOC Services

<table>
<thead>
<tr>
<th>Hours of Service</th>
<th>SKU</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 hrs Per SKU</td>
<td>F5-FAS-SOCS-20H-1Y</td>
</tr>
<tr>
<td>40 hrs Per SKU</td>
<td>F5-FAS-SOCS-40H-1Y</td>
</tr>
<tr>
<td>60 hrs Per SKU</td>
<td>F5-FAS-SOCS-60H-1Y</td>
</tr>
<tr>
<td>80 hrs Per SKU</td>
<td>F5-FAS-SOCS-80H-1Y</td>
</tr>
</tbody>
</table>

Recommended SOC Service SKUs based on sites/bandwidth

### Upgrades

<table>
<thead>
<tr>
<th>Additional Bandwidth</th>
<th>1YR SKU</th>
<th>3YR SKU</th>
<th>Additional Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5-FAS-WAF-ADD-50M1Y</td>
<td>F5-FAS-WAF-ADD-50M3Y</td>
<td>Add 50 Mbps/month</td>
<td></td>
</tr>
<tr>
<td>F5-FAS-WAF-ADD100M1Y</td>
<td>F5-FAS-WAF-ADD100M3Y</td>
<td>Add 100 Mbps/month</td>
<td></td>
</tr>
<tr>
<td>F5-FAS-WAF-ADD500M1Y</td>
<td>F5-FAS-WAF-ADD500M3Y</td>
<td>Add 500 Mbps/month</td>
<td></td>
</tr>
<tr>
<td>F5-FAS-WAF-ADD-1G-1Y</td>
<td>F5-FAS-WAF-ADD-1G-3Y</td>
<td>Add 1 Gbps/month</td>
<td></td>
</tr>
</tbody>
</table>

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

### Additional Sites

<table>
<thead>
<tr>
<th>Additional Sites</th>
<th>1YR SKU</th>
<th>3YR SKU</th>
<th>Additional Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add 5 Sites</td>
<td>F5-FAS-WAF-ADD-5S-1Y</td>
<td>F5-FAS-WAF-ADD-5S-3Y</td>
<td>Add 5 Sites</td>
</tr>
<tr>
<td>Add 10 Sites</td>
<td>F5-FAS-WAF-ADD-10S1Y</td>
<td>F5-FAS-WAF-ADD-10S3Y</td>
<td>Add 10 Sites</td>
</tr>
<tr>
<td>Add 50 Sites</td>
<td>F5-FAS-WAF-ADD-50S1Y</td>
<td>F5-FAS-WAF-ADD-50S3Y</td>
<td>Add 50 Sites</td>
</tr>
<tr>
<td>Add 100 Sites</td>
<td>F5-FAS-WAF-ADD100S1Y</td>
<td>F5-FAS-WAF-ADD100S3Y</td>
<td>Add 100 Sites</td>
</tr>
</tbody>
</table>

Contact your F5 Channel Account Manager for more information.
Template Recommendations
9 Common Mistakes to Avoid in Your Presentation

1. **On-premises**, not on-premise. One is not the plural of the other— they are not interchangeable, but two completely different words. A premise is a proposition, whereas a premises is a tract of land.

2. **BIG-IP**. All caps, with hyphen. Not Big-IP, BIG IP, Big IP, or any other variation.

3. **BIG-IP DNS**. Not BIG-IP Global Traffic Manager or BIG-IP GTM.

4. **BIG-IQ**. All caps, with hyphen. Not Big-IQ, BIG IQ, Big IQ, or any other variation.


7. **No trademarks necessary**. You do not need to include any trademarks in your presentations—please strip them all out.

8. **Size matters**. If the font size is too small for your audience to read, it’s worthless.

9. **Don’t forget spell-check**. It’s free, it’s fast, it can save you face.

You can find the complete F5 Content Style Guide [here](#).

Questions? Contact [Jenn League](#) any time.
Template Tutorial Video

We have put together a brief video tutorial on the Agility 2016 PowerPoint Template.

PASSWORD: agility

LINK TO VIEW VIDEO
https://vimeo.com/f5networks/review/158553936/d3a47cc04c

0:00-03:40
Walk-through of the template contents and recommendations.

03:40-10:47
Demo on transferring your existing slides into the Agility 2016 PowerPoint Template
Turning on the Header & Footer

1. Go to the **Insert** tab, and click on **Header & Footer**.

2. You will get a pop-up box. Make sure the **Slide** tab is selected and not the Notes & Handouts tab.

3. Make sure to the **Slide number**, **Footer**, and **Don’t show on title slide** boxes are all checked.

4. Select **Apply to All**
   *Note if you choose **Apply** it will only apply to that single slide.*
Preferred Text Layout (No Bullets)

Main Topic 1: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 2: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 3: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics
Preferred 2-Column Text Layout (No Bullets)

Main Topic 1: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 2: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 3: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 4: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 5: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 6: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics
Preferred Text Layout with Sub-Header

Sub-header

Main Topic 1: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 2: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 3: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics
## Preferred 2-Column with Sub-Header (No Bullets)

**Sub-header**

<table>
<thead>
<tr>
<th>Main Topic 1: Size 32pt</th>
<th>Main Topic 4: Size 32pt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size 24 for the sub topics</td>
<td>Size 24 for the sub topics</td>
</tr>
<tr>
<td>Size 24 for the sub topics</td>
<td>Size 24 for the sub topics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Main Topic 2: Size 32pt</th>
<th>Main Topic 5: Size 32pt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size 24 for the sub topics</td>
<td>Size 24 for the sub topics</td>
</tr>
<tr>
<td>Size 24 for the sub topics</td>
<td>Size 24 for the sub topics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Main Topic 3: Size 32pt</th>
<th>Main Topic 6: Size 32pt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size 24 for the sub topics</td>
<td>Size 24 for the sub topics</td>
</tr>
<tr>
<td>Size 24 for the sub topics</td>
<td>Size 24 for the sub topics</td>
</tr>
</tbody>
</table>
SECTION TITLE HERE
Your famous, remarkable, quote goes here. **You can use bold to create emphasis.**

Author’s Name (Arial 24pt, spacing condensed by 1pt)
This is an example of a data point slide that has been enhanced with line icons. Line icons can also be used to highlight benefits.

See slides 35–39 for icons.
Example Horizontal Bar Chart

Charts are editable. Right-click on chart and select Edit Data.
Example Percentage Charts

Charts are editable. Right-click on chart and select Edit Data.
Example Pie Chart

Charts are editable. Right-click on chart and select Edit Data.
Example Diagram

- Users
- Attackers
- Office 365
- Google Apps
- Salesforce
- SaaS Providers
- SAML: Real-time access control, Access policy enforcement
- Corporate Users
- Access Management
- Directory Services
- Corporate Applications
- On-Premises Infrastructure
- Identity federation
- Strategic Point of Control
- Multi-factor authentication
SOLUTIONS FOR AN APPLICATION WORLD
Preferred Text Layout (No Bullets)

Main Topic 1: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 2: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 3: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics
Preferred Text Layout with Sub-Header

Sub-header

Main Topic 1: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 2: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 3: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics
Sub-header

Main Topic 1: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 2: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 3: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 4: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 5: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics

Main Topic 6: Size 32pt
Size 24 for the sub topics
Size 24 for the sub topics
SECTION TITLE HERE
Your famous, remarkable, quote goes here. **You can use bold to create emphasis.**

Author's Name (Arial 24pt, spacing condensed by 1pt)
This is an example of a data point slide that has been enhanced with line icons. Line icons can also be used to highlight benefits. See slides 35–39 for icons.
Example Horizontal Bar Chart

Charts are editable. Right-click on chart and select Edit Data.
Example Percentage Charts

Charts are editable. Right-click on chart and select Edit Data.
ICONS: For Data Visualization
ICONS:
For Diagrams
F5 software and services

- LTM [BIG-IP Local Traffic Manager]
- DNS [BIG-IP DNS]
- AAM [BIG-IP Application Acceleration Manager]
- AFM [BIG-IP Advanced Firewall Manager]
- APM [BIG-IP Access Policy Manager]
- ASM [BIG-IP Application Security Manager]
- LINK [BIG-IP Link Controller]
- PEM [BIG-IP Policy Enforcement Manager]
- CGNAT [BIG-IP Carrier-Grade NAT]
- SDC [Signaling Delivery Controller]
- BIG-IQ [BIG-IQ]
- EM [Enterprise Manager]
- WEBSAFE [WebSafe]
- MOBILESAFE [MobileSafe]
- SWG [Secure Web Gateway Services]
- IP [IP Intelligence]

Application Examples

- Silverline
  - F5 Silverline Cloud-Based Services
- LineRate
  - POINT-LB [LineRate Point Load Balancer]
  - PREC-LB [LineRate Precision Load Balancer]
F5 software—virtual editions

Use the smaller VE icon when representing a specific F5 virtual edition.

When the use case calls for a “and/or” representation (F5 hardware and/or F5 VE) use this larger VE icon. Use the same VE icon within a given diagram—don’t mix and match.

Example of functionalities

VE icon has a white outline

© 2016 F5 Networks
F5 product representation

To represent F5 or third-party hardware, you can choose from the options below. When deciding which to use, consider how much information your audience needs.
F5 product representation—options

- **Load Balancing**
- **DDoS Protection**
- **Firewall**

**BIG-IP Platform**

**VIPRION Platform**

**Devices**

**Internet**

**Data Center**

**BIG-IP Local Traffic Manager (LTM)**

**BIG-IP Access Policy Manager (APM)**

**BIG-IP Application Security Manager (ASM)**

© 2016 F5 Networks
Hardware user devices

- **Desktop**
  - Desktop
  - Desktop E-Commerce
  - Desktop Reporting

- **Laptop**
  - Laptop
  - Infected Laptop
  - Mobile Hotspot

- **Phone**
  - Smartphone
  - With Authentication
  - Mobile Hotspot

- **Tablet**
  - Tablet
  - Tablet with Apps
  - Passcode
  - Tablet with Collaboration
  - Mobile Hotspot
Hardware user devices—options

Clustered Groupings

Horizontal Groupings

Vertical Groupings
Network hardware

Server
Servers
Servers
Servers
Server
Classic Server
Blade Server
Server Rack
Storage
Database
Data

Public Cloud
Private/Public Cloud
Hybrid Cloud
Private Cloud
Internet
CPU

WAN
Router
Switch
ADC
Firewall
IaaS
SaaS
PaaS
Service provider-specific

Support Nodes
- SGSN
- GGSN/PGW
- SGW
- PGW
- GGSN/PGW/ASNGW

Policies or Functions
- PCRF
- v-PCRF
- h-PCRF
- OCS
- SIP AS

Control Nodes
- MME
- Access Node

Databases
- HSS
- Active Directory

Alternate Routers
- PE
- IGR
- DEA
- Roaming Hub

Networks and Protocols
- Diameter
- HTTP
- S6a
- DSL
- LDAP
- S8
- Cable
- Logging Mirror Access
- S9
- FTTH
- Lu-PS
- SGI
- Gb
- MAP
- SIP
- GI
- OpenStack API
- SIP
- GI
- SOAP
- GI
- RADIUS
- SS7
- Rx
- GTP
- S1
- Gx/Sd
- S11
- Gx/Sd
- S11
- Gy
- XML
- Gx/Sd
- XML
- x-CSCF
- [network]
Virtual instances

The Hypervisor label is used for generic hypervisors, to be more specific replace the label with a brand name product:

- Hyper-V
- KVM
- vSphere
- Xen
General

Security
- Attacker
- Attackers
- Web Bot
- Shield
- ID Tag
- Authentication

Technology solutions
- Provisioning
- DDoS Protection
- Data Migration
- Tiering
- Security
- WAN Optimization
- Local Load Balancing
- Global Load Balancing
- Link Load Balancing

Users/ Admin
- User
- User 2
- Admin
- Unidentified User
- Alternative User
- Alternative User
Small icons

Place these small icons directly on top of connecting lines to help tell the story. In general, these icons don’t need labels.

| Unsecure | Secure | No Entry | Approved | Not Approved |

Use these small icons can be placed on larger icons to change their state.

| Certified | Tokenized |

Use the bracket and smaller text box to describe what’s going on in more detail.

} More information and details.  

} Even more information and details.  

} And even more information and details. Always center text to bracket.