



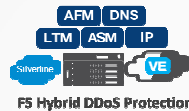
DDoS Protection: Quick Reference Card

What is it?	Why Customers Buy?	Quick Market Facts
<p>Distributed Denial of Service (DDoS): DDoS is a type of cyber attack that leverages multiple compromised systems, often infected with a Trojan, and used to target a single system causing a Denial of Service (DoS) attack.</p> <p>DDoS Protection Solutions: Technologies designed to detect, prevent and contain DDoS attacks. Most common include: cloud scrubbing, ISP services, end-point security, firewalls, and network/traffic intelligence solutions. Demand for hybrid solutions that leverage both physical devices and cloud-based services is increasing.</p>	<ul style="list-style-type: none"> Protect Brand: With major outages making monthly headline news, customers are eager to reduce the cost and damage of these attacks to their brand and business. Financial Impact: According to a 2015 Ponemon report, the average total cost per year to deal with DoS is approximately \$1.5 million. This includes lost productivity, disruption to operations, damage to infrastructure, and loss of revenue. Compliance Purposes: Organizations that handle or transact sensitive data, often in the financial, health and government verticals, are required to implement federal policies intended to help mitigate cyber attacks (PCI, Sarbanes-Oxley, HIPAA) Future Proofing: Customers are looking to strengthen their IT security now rather than pay the much higher costs associated with cleaning up and recovering from a successful DDoS attack. 	<ol style="list-style-type: none"> 10-12 % growth projected for cloud security services through 2018 \$52k-\$400k/hr. is the cost of a single DDoS attack on a SMB or Enterprise (2014 Kaspersky Lab Report: Global Corp IT Security Risks) 9 hours per year and 54 min per successful DDoS attack is the avg. downtime (Ponemon Institute 2014 and 2012) In 2014 there were 1.5 million, monitored cyber attacks in the US alone. (2014 Cyber Security Intelligence Index) Barriers to preventing DDoS insufficient budget (49%) and lack of qualified security personnel (46%) 2015 Ponemon

F5 DDoS Protection Offerings

Hybrid DDoS Protection:

Integrates BIG-IP on-premises protection with Silverline cloud-based scrubbing for full DDoS coverage and high mitigation capacity for the datacenter



BIG-IP ASM

Application Attacks:
HTTP flood + Recursive GET + Slowloris + Brute force



BIG-IP LTM

SSL Attacks:
SSL flood + SSL Intercept
SSL renegotiation



BIG-IP DNS

DNS Attacks:
UDP flood + NXDOMAIN query flood + NS query flood



BIG-IP LTM + BIG-IP AFM + IPI

Network Attacks:
SYN flood + Connection flood + UDP flood + ICMP flood



Cloud-based DDoS Protection:

F5 Silverline™ DDoS Protection is a fully managed service that augments resources for DDoS mitigation

Managed Service



Cloud-based, Enterprise Grade, L3-L7 DDoS Protection

- Managed Service:** the industry's most responsive 24/7 SOC
- Expert Resources:** access to the world's foremost DDoS experts
- Transparent Operations:** immediate visibility into all SOC actions and threats
- Extensible Solution:** Integrates with F5 on-premises AFM & ASM
- Protects Datacenter:** defends against the largest DDoS attacks without regard for ISP, Origin

F5 Security Operations Center



How to Sell Your Customers DDoS Protection

1 Identify your target customer

EXECUTIVE LEADER	SECURITY / NETWORK VP, DIR., ARCH.	SECURITY / NETWORK ENGINEER	APPLICATION OWNER
<p>Key Responsibilities:</p> <ul style="list-style-type: none"> Delivers new systems and architectures within fixed IT budget. Expands business growth and strategic impact. <p>Talking Point Interests:</p> <ul style="list-style-type: none"> How not to be the next front page security breach Innovation with larger industry trends (e.g. IoT, Cloud, IPaaS) Protecting company brand, assets and revenue from an IT perspective (High level decision maker) Increasing the ROI of IT 	<p>Key Responsibilities:</p> <ul style="list-style-type: none"> Makes key IT architectural decisions Balance business needs with security needs Designs security architecture implementations and responsible security services <p>Talking Point Interests:</p> <ul style="list-style-type: none"> Ways to reducing IT OPEX New IT architectural innovation Hybrid or managed service technology and impacts to business Architectures for an extended enterprise and complex, multi-vendor environment Concerned with scalability, agility 	<p>Key Responsibilities:</p> <ul style="list-style-type: none"> Initial, upgrade and maintains app/network security Works with cross functional IT and LDB teams to plan large-scale system implementations Secures complex apps and cloud environments Speeds app deployments/upgrades and simplifies management <p>Talking Point Interests:</p> <ul style="list-style-type: none"> Orchestration and automation around deploying IT infrastructure Ways increase App protection, deployment agility and scalability 	<p>Key Responsibilities:</p> <ul style="list-style-type: none"> Create, deploy and support applications for end users Ensure applications and supporting services operate as expected and securely Collaborate with Network, security and IT teams to plan implementations and deployments <p>Talking Point Interests:</p> <ul style="list-style-type: none"> Ways to reduce time to deploy DevOps Innovation (i.e. whatever makes developing, deploying and securing apps easier)

2 Determine the right solution

Critical Question: Do you have resources/expertise to mitigate DDoS attacks?

Other Key Points To Consider With Your Target Customers	Hybrid DDoS	Silverline WAF
Needs to maintain DDoS policy control	✓	
Concerns about volumetric attacks	✓	✓
Concerns about sophisticated app layer attacks	✓	
Consolidating data center infrastructure protection		✓
Refreshing or strengthening existing datacenter devices	✓	✓
Needs to ensure app servers are always up	✓	✓
Demands high mitigation capacity	✓	✓
Lacks specialized resources for DDoS mitigation		✓
Prefer outsourcing DDoS security		✓
Require 24x7x365 attack support and security expertise	✓	✓

3 Sell the full DDoS Portfolio

- Sell beyond basic DDoS protection
- Emphasize value of IP intelligence and Silverline services for complete hybrid solution