Firewall Fail: Live Next-Gen Firewall Testing to Expose Breaking Points

Mike Hamilton

BreakingPoint Systems

Session ID: SPO2-301

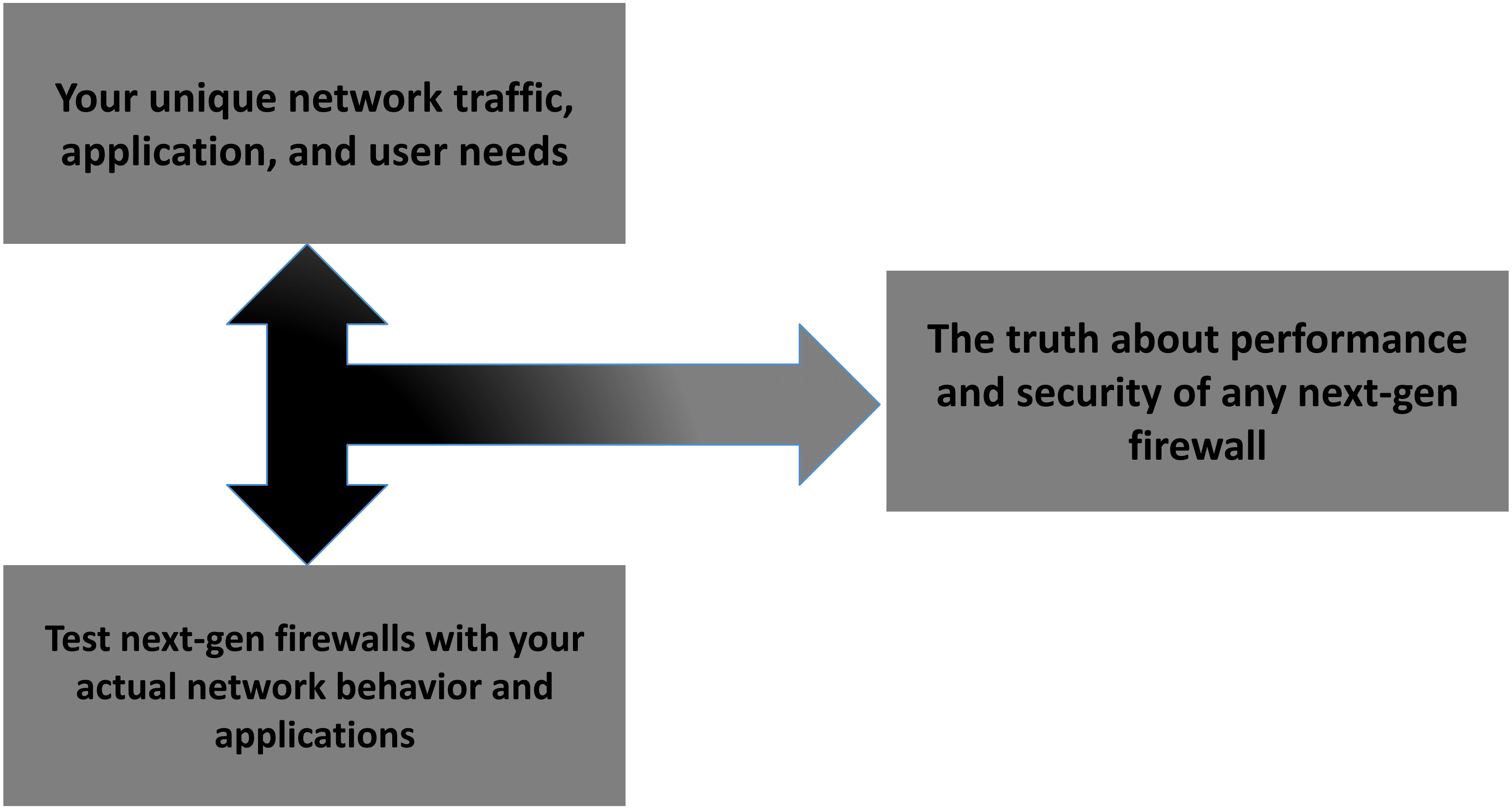
Session Classification: Advanced

RSACONFERENCE2012

Agenda & Introduction

- **Today's Speaker:**
  - Mike Hamilton – Director of Global Sales Engineering
    - mhamilton@breakingpoint.com
- **Today's Topics:**
  - Why next-generation firewalls?
  - The truth about testing next-generation firewalls
  - Three Truths to get you started
  - Live test of a next-generation firewall

The Truth Hurts: Find It Before They Do



Your unique network traffic, application, and user needs

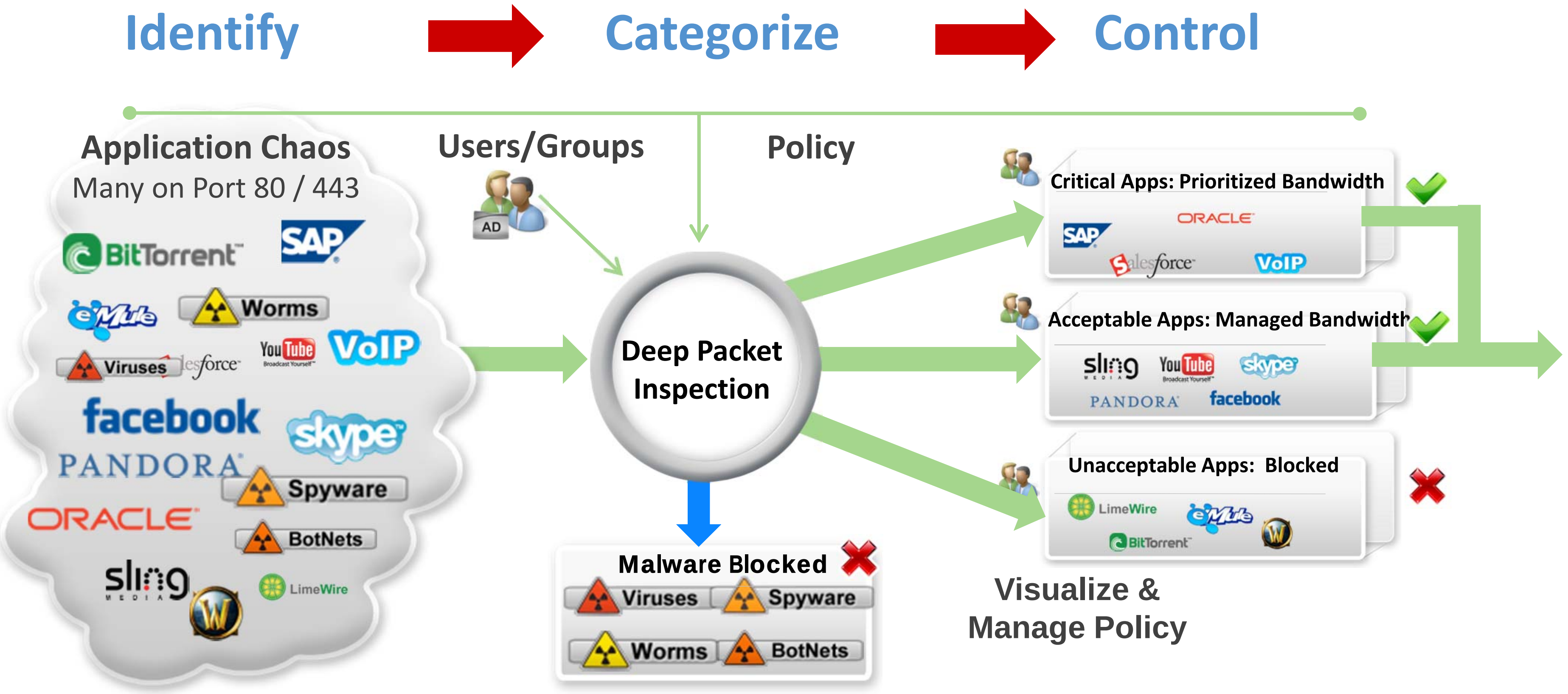
The truth about performance and security of any next-gen firewall

Test next-gen firewalls with your actual network behavior and applications

Today You Will Learn:

- Three mistakes in testing next-gen firewalls that will lead to failures
- How to stay ahead of testing standards in order to measure the true performance of a next-generation firewall
- The best way to choose a next-gen firewall for your unique application, security, and capacity needs

Why Deploy Next-Generation Devices?



Identify → Categorize → Control

Application Chaos
Many on Port 80 / 443

Users/Groups

Policy

Deep Packet Inspection

Malware Blocked

Critical Apps: Prioritized Bandwidth

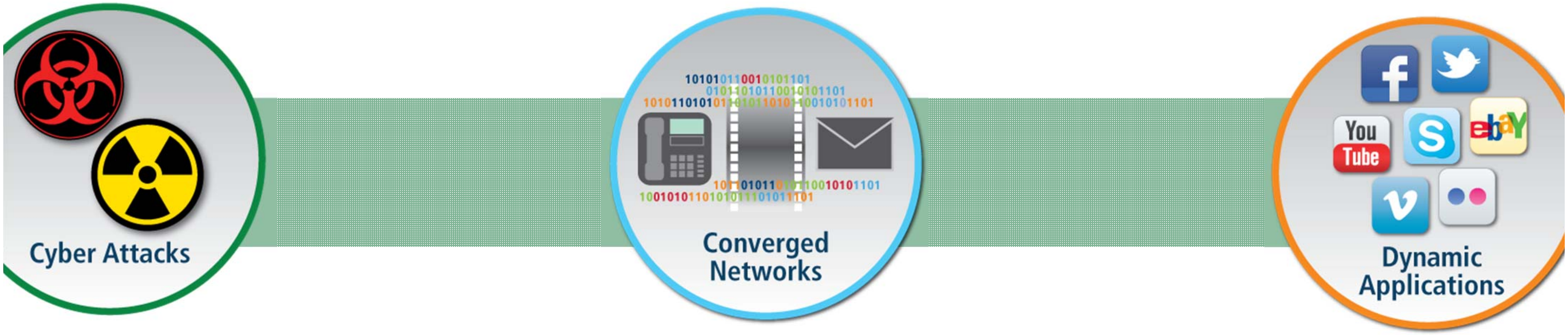
Acceptable Apps: Managed Bandwidth

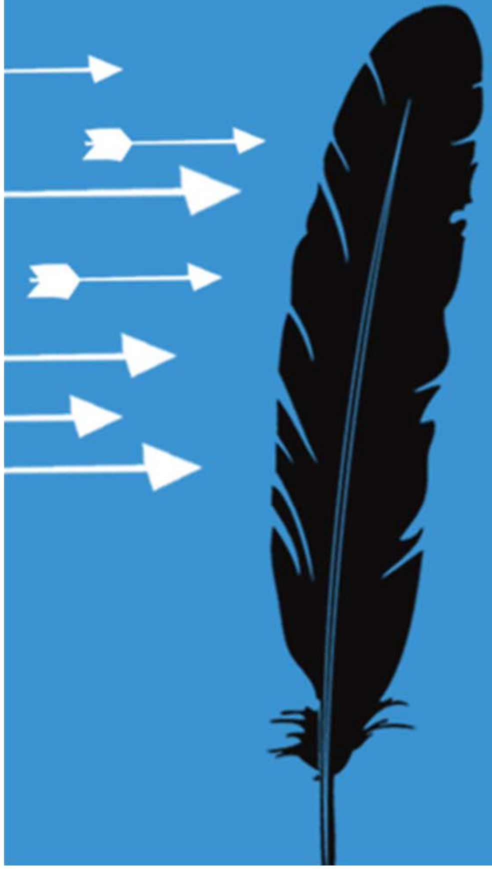
Unacceptable Apps: Blocked

Visualize & Manage Policy

Next-Gen Firewall Demands Next-Gen Testing

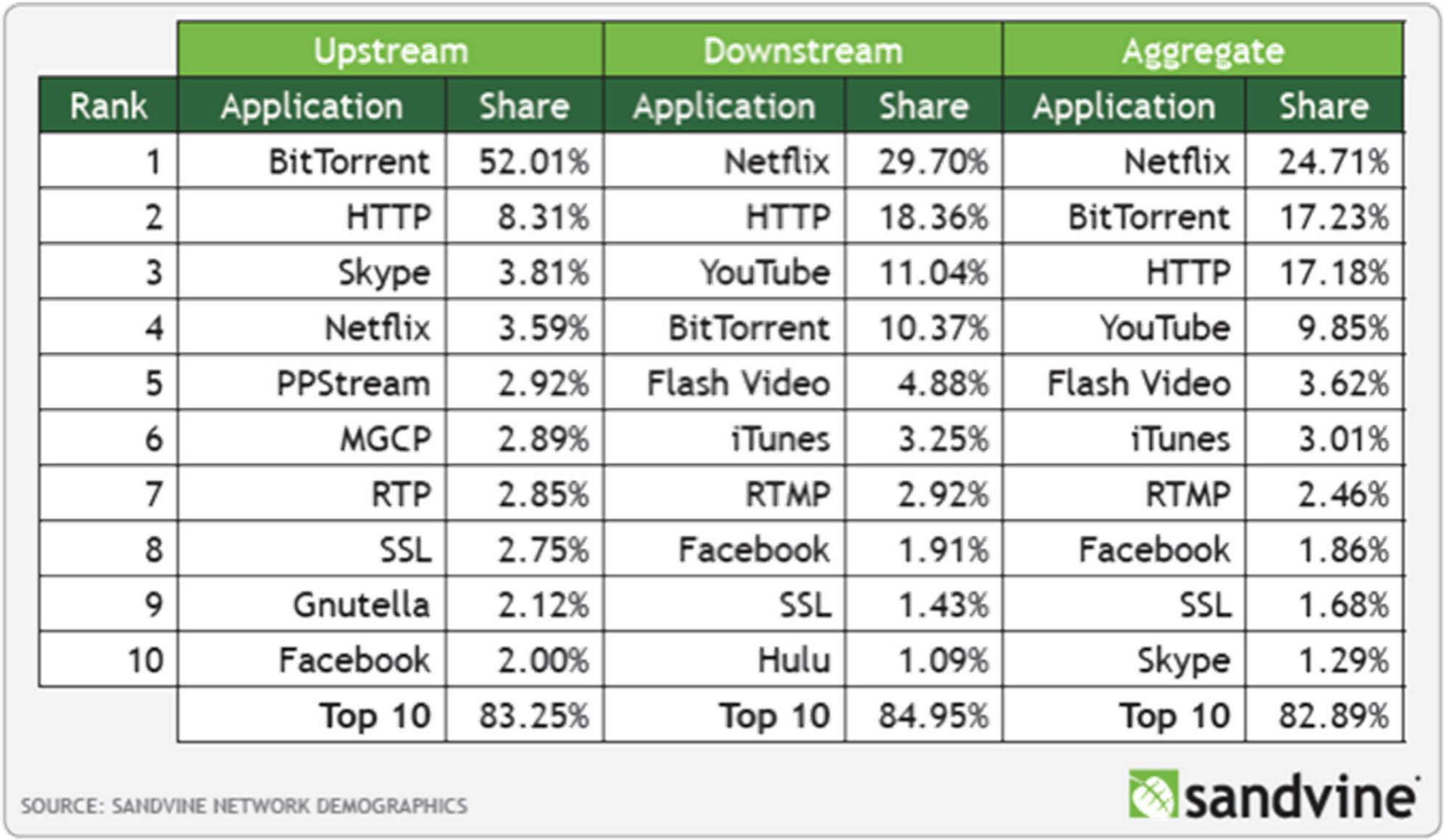
- Application identification
- Application access control
- Application QoS
- Application-layer attack
- SSL/TLS inspection
- Malware filtering





Three Initial Truths…

Truth 1: HTTP Is NOT an Application



	Upstream		Downstream		Aggregate	
Rank	Application	Share	Application	Share	Application	Share
1	BitTorrent	52.01%	Netflix	29.70%	Netflix	24.71%
2	HTTP	8.31%	HTTP	18.36%	BitTorrent	17.23%
3	Skype	3.81%	YouTube	11.04%	HTTP	17.18%
4	Netflix	3.59%	BitTorrent	10.37%	YouTube	9.85%
5	PPStream	2.92%	Flash Video	4.88%	Flash Video	3.62%
6	MGCP	2.89%	iTunes	3.25%	iTunes	3.01%
7	RTP	2.85%	RTMP	2.92%	RTMP	2.46%
8	SSL	2.75%	Facebook	1.91%	Facebook	1.86%
9	Gnutella	2.12%	SSL	1.43%	SSL	1.68%
10	Facebook	2.00%	Hulu	1.09%	Skype	1.29%
	Top 10	83.25%	Top 10	84.95%	Top 10	82.89%

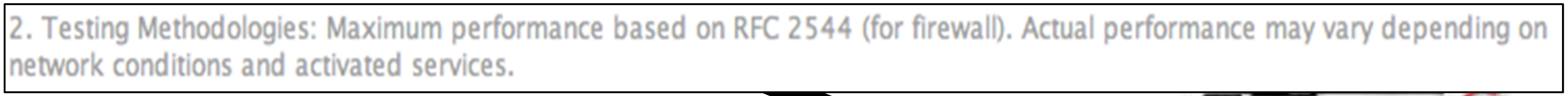
SOURCE: SANDVINE NETWORK DEMOGRAPHICS

sandvine

Truth 2: Today’s Applications/Threats Will Change

- New applications introduced each day
  - Constant changes to popular applications such as email, IM, etc.
- New threats introduced each day
  - Vulnerabilities
  - DDoS evolution
  - Malware
- New devices introduced each day
  - Mobile malware
  - Wireless to wired traffic

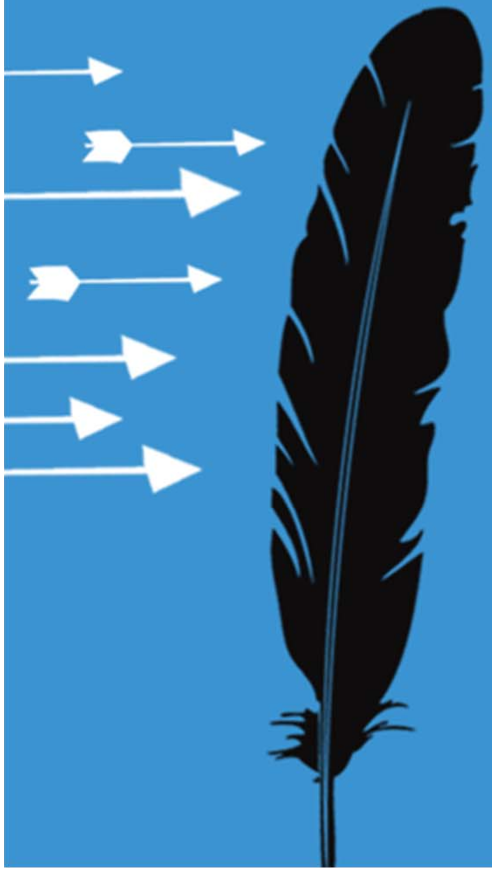
Truth 3: RFC 2544 Is A Fossil



2. Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

- Dated benchmarking methods:
  - Vendors use to inflate performance numbers
  - Misleading security and performance data can lead to failure

- Use forward-thinking methodologies
  - Stay ahead of the curve
  - IETF standards are evolving



LIVE TESTING: Finding the truth

Wrap It Up: Six Questions To Find The Truth

- Ask your vendor*:
  1. Are you keeping up with emerging testing standards?
  2. What application mixes and weights do you use during testing?
  3. Do you combine applications and high-stress user load during testing?
  4. What have the results been when you have tested using malformed traffic?
  5. How does the firewall perform against application-layer attacks?
  6. Can I test your product with my unique network, application, and user conditions?

*Vendors, ask yourself the same questions.

Q & A