RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

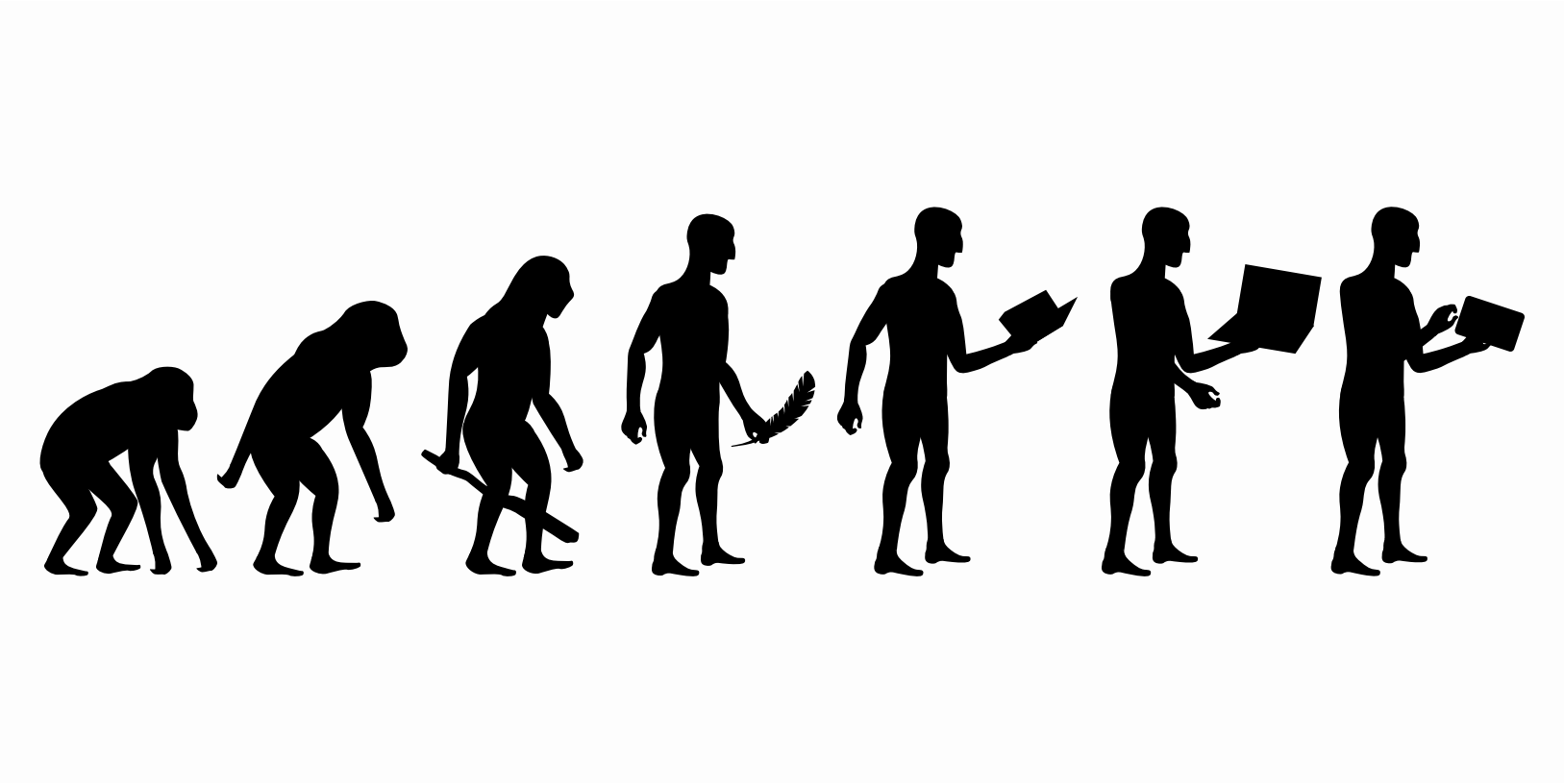
SESSION ID: SPO3-T11

Application and Threat Intelligence: Driving Security Offense and Defense

Glenn Chagnot
Senior Director of Product Management, Ixia
@Ixia_ATI

Steve McGregory
Director of ATI Research Center, Ixia

We've Evolved?



Changing Every Day

IPv6
LTE – 5G
New Apps
SSL
Cloud
Content Centric Networking

All of these add new code/libraries, bugs, and more opportunity for hackers

Attacks Evolved?

Morris Worm
Buffer Overflow

CVE-2016-1287
Buffer Overflow

1988 — 2016

We're still introducing the same old bugs in our code

DEP & ASLR makes exploitation more difficult

Plenty of programs/libraries/systems still not supporting ASLR/DEP

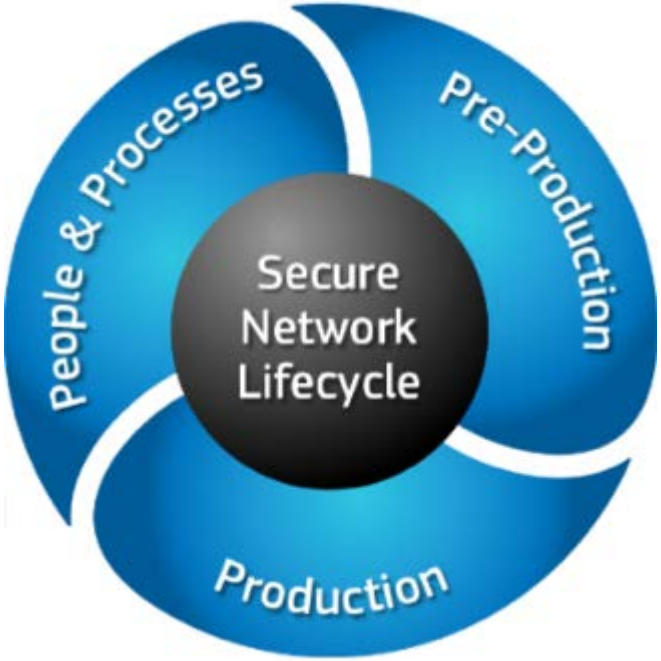
Intro – Application and Threat Intelligence

Application and Threat Intelligence (ATI)

- Application
  - Transports
  - Protocols/Apps
- Threat
  - Attacks/Vulns
- Intelligence
  - Bad Actors
  - Techniques

ATI Applied to Lifecycle

360 Degree Security for Your Network



Lifecycle Validation

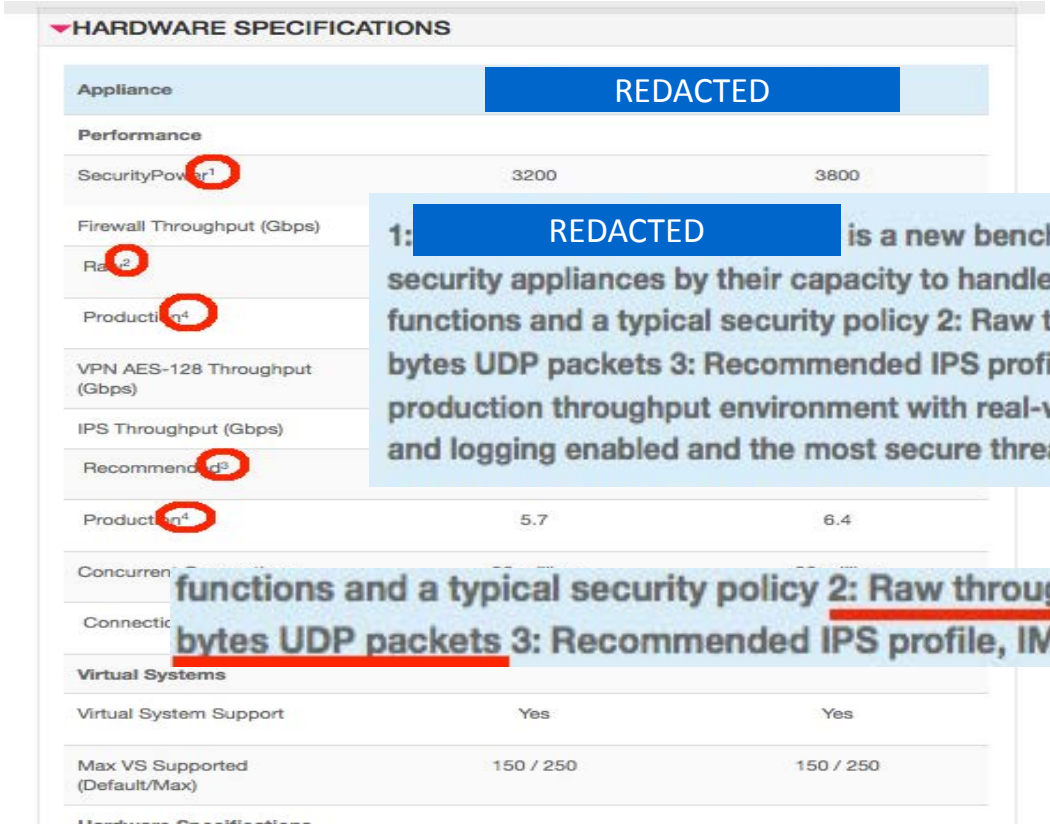
Pre-Production/Production Validation

Do you trust the vendor data sheets?

They are correct, but…

Disclaimer: No vendor bashing meant, they all do it

Vendor data sheets, downhill, wind at back…



HARDWARE SPECIFICATIONS

Appliance	REDACTED	
Performance		
SecurityPower[1]	3200	3800
Firewall Throughput (Gbps)		
Raw[2]		
Production[4]		
VPN AES-128 Throughput (Gbps)		
IPS Throughput (Gbps)		
Recommended[3]		
Production[4]	5.7	6.4
Concurrent		
Connections		
Virtual Systems		
Virtual System Support	Yes	Yes
Max VS Supported (Default/Max)	150 / 250	150 / 250

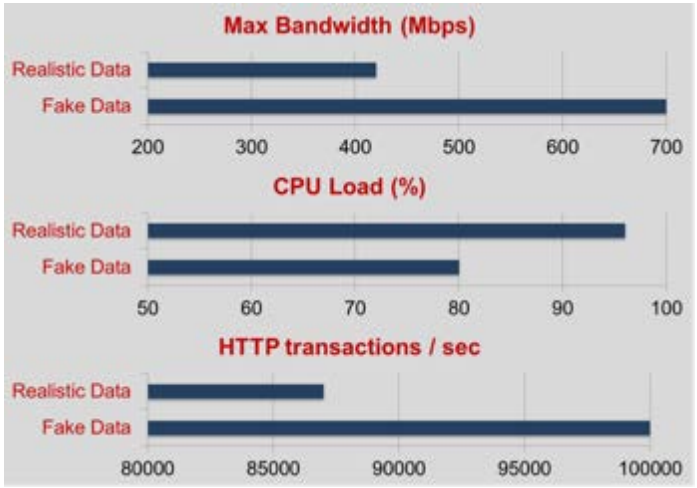
REDACTED

1: is a new benchmark metric that allows customers to select security appliances by their capacity to handle real-world network traffic, multiple security functions and a typical security policy 2: Raw throughput is based on RFC 3511 with 1518 bytes UDP packets 3: Recommended IPS profile, IMIX traffic blend 4: Assumes maximum production throughput environment with real-world traffic blend, a typical rule-base size, NAT and logging enabled and the most secure threat prevention protection

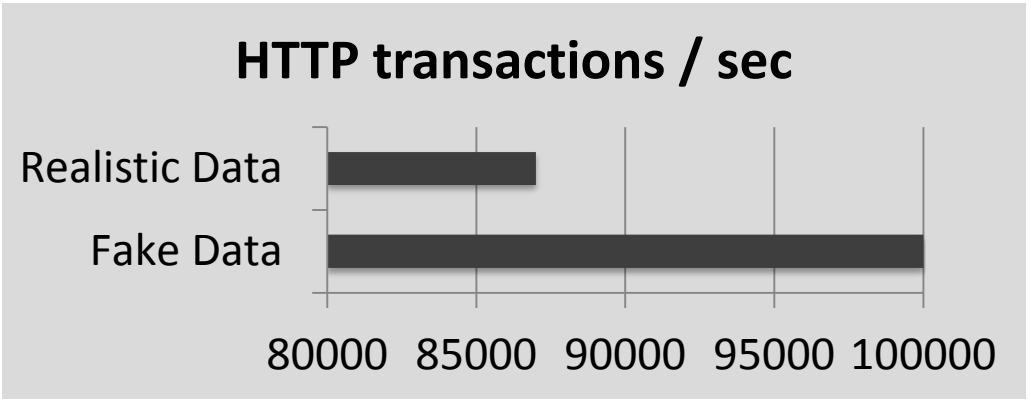
functions and a typical security policy 2: Raw throughput is based on RFC 3511 with 1518 bytes UDP packets 3: Recommended IPS profile, IMIX traffic blend 4: Assumes maximum

Content impacts DPI performance

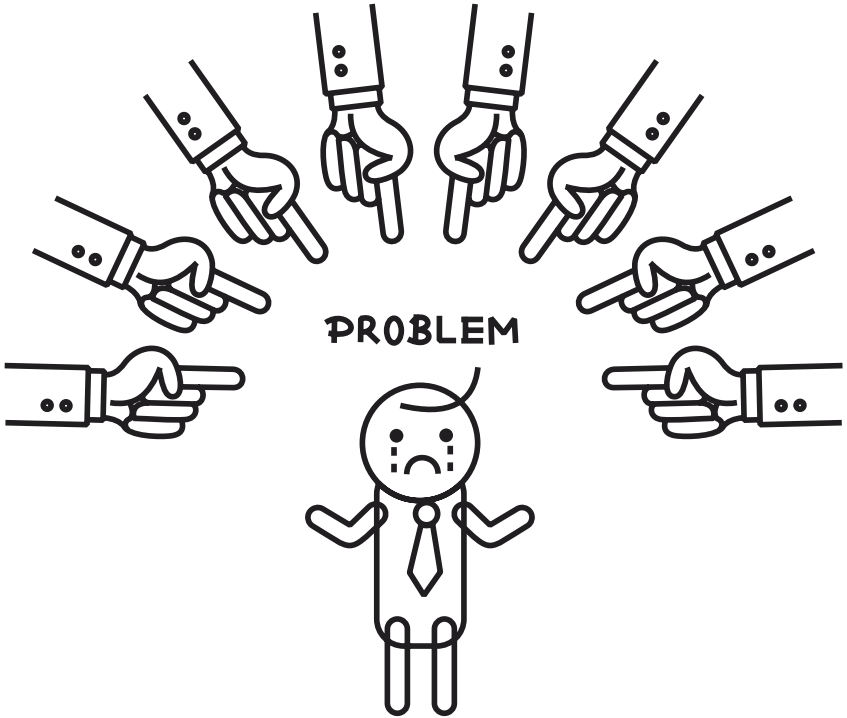
Proxy Device



NGFW with IPS



Why do you care?



Time for a Story

There once was a man from Nantucket…

Have you heard this one before?

He was saved by testing an update before applying to production!

Customer Use Case

Product Evaluation – Multinational Corporation

Customer

- 100,000 Employees
- Focused on energy, consumer, and finance

Need

- Maximizing reliability of network upgrades
- Ensure “No Surprises”

Results

- Customer was able to avoid a patch that would have reduced performance by 80%

Security Product Evolution

More Evolution: Security Products

Firewalls

Evaded

More Evolution: Security Products

DPI – IPS/NGFW

Evaded

More Evolution: Security Products

DPI – IPS/NGFW
Sandboxing

Evaded

Security is a process

Products provide some protection

Reduce risk of exposure

Don’t be the low hanging fruit

Lifecycle: Production/People Processes

Are you a control freak?

- You cannot control all the code
- You cannot control weakness in Security products

You can control…

- Noise by Reducing Alerts through…
- Reduced Attack Surface
- Access to/from Known Malicious Systems

Network Visibility

Knowing What's In Your Network

What next?

You are validating

- Pre-Production – Data Sheet Validation
- Production – Patch/Update Validation
- People/Processes – Optimizing, lowering noise/surface

You Are No Longer
Low Hanging Fruit

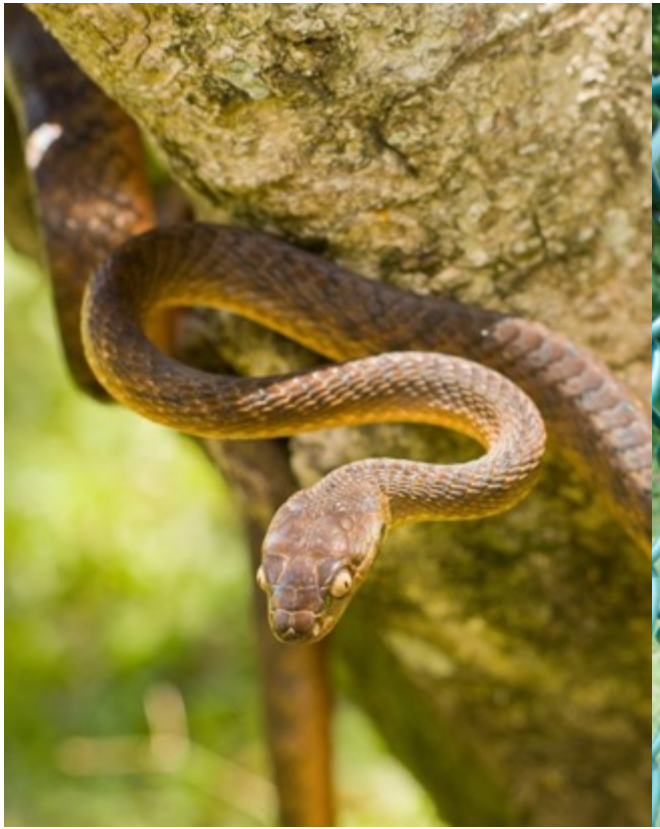
The Targeted Attack

The dreadful targeted attack:
“Lieutenant, your men are already dead”

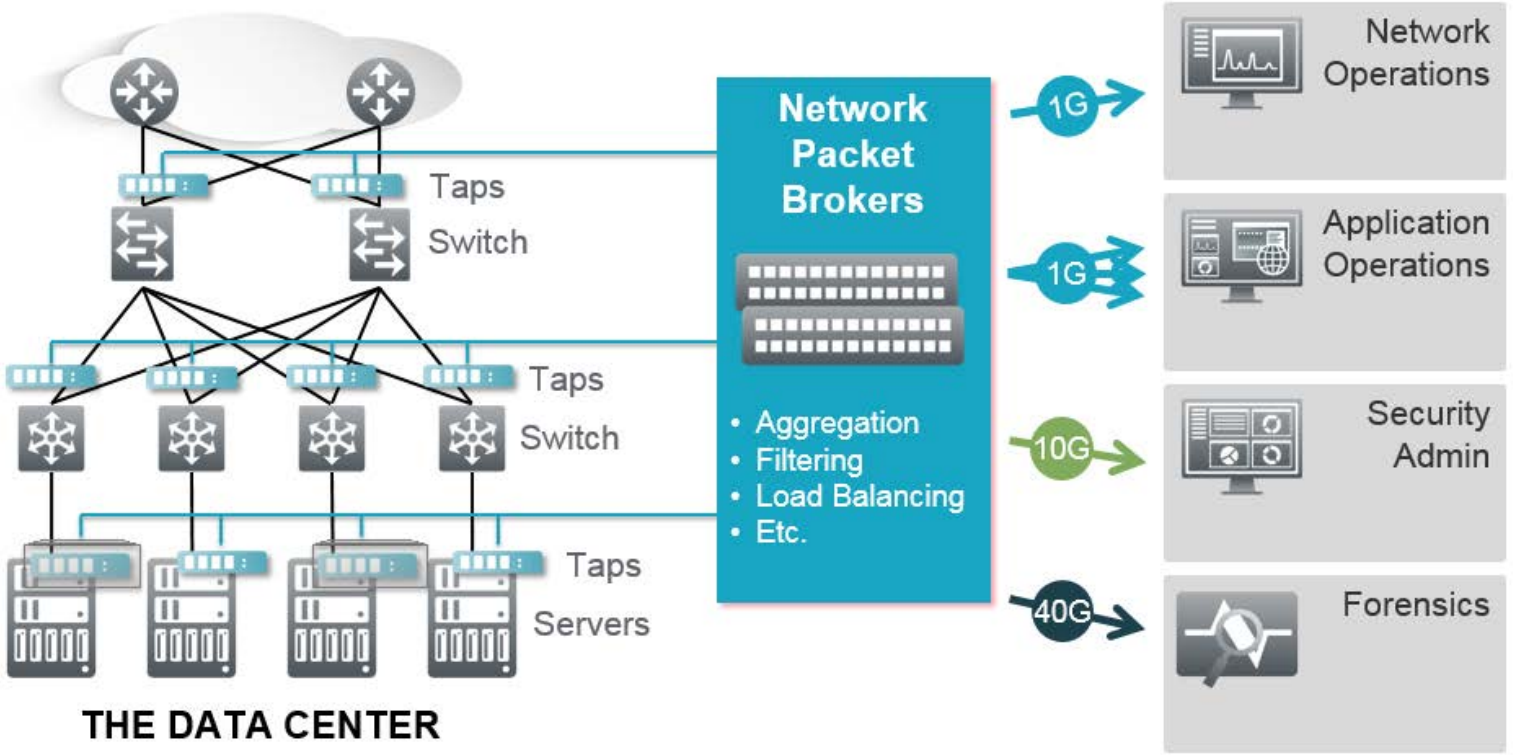
50%
Phishing emails opened and clicked within first hour

Avg. 229 Days
Compromise goes without notice

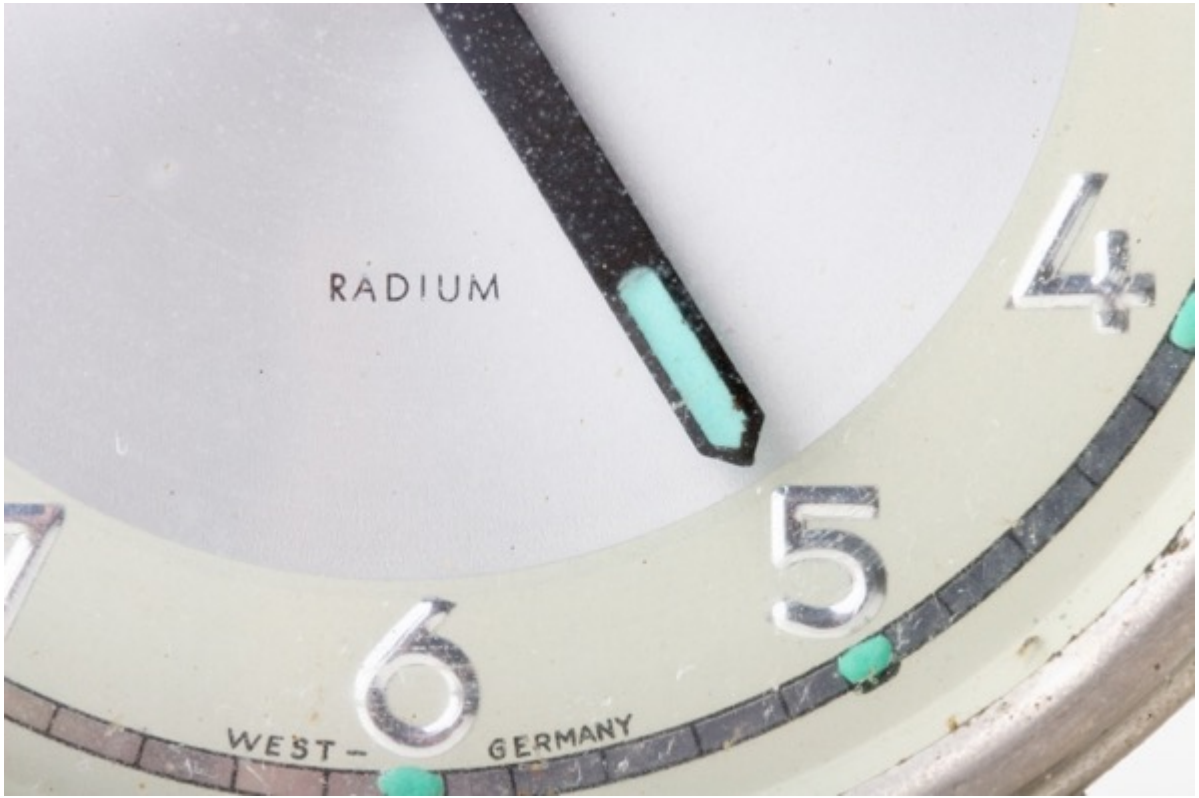
Edge versus Core



Security Architecture

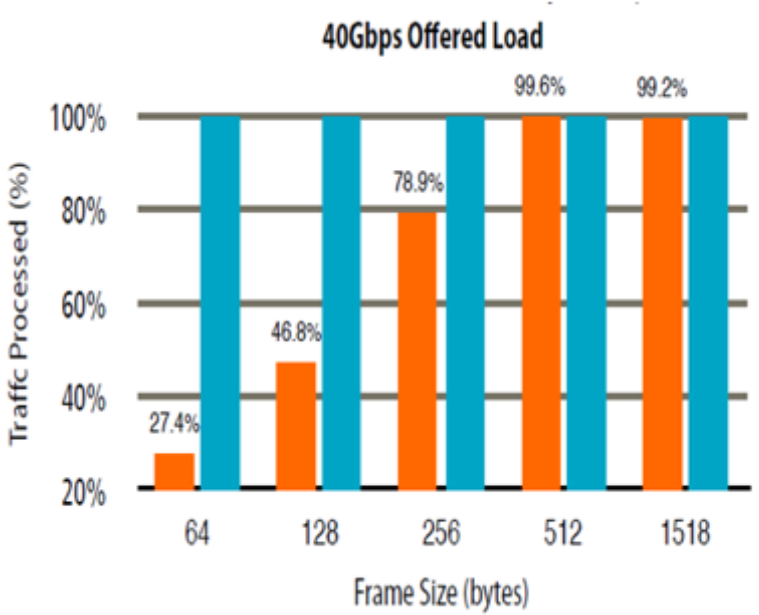


What is Worse than No Data?



Find Out Before They Do

- Visibility Architecture Matters
  - Taps vs SPANs
  - Decryption support
  - NPB performance
  - IDS performance
- What is the impact?
  - Nearly 50% more threats went undetected by IDS
  - Specific to the deployment
  - Test it yourself!



Next Steps

Next Steps - Evolve

- Don’t just trust, but verify
  - Design full security architecture, don’t just focus on the analysis tools
  - Validate products, processes
- Lower your
  - Attack surface
  - Noise operations must deal with everyday
- Don’t be the low hanging fruit
- Know what’s in your network, and lessen time to detect compromises

Thank You – Q&A?

Glenn Chagnot – Senior Director of Product Management

Steve McGregory – Director of ATI Research Center
@Ixia_ATI

Booth #3201 in the North Hall