How to build a Carrier-Grade Defense-Shield

Dr. Antonio Nucci

Chief Technology Officer, Narus Inc.

Agenda

NARUS®

- Security Market Landscape
- Approach to Efficiently and Shortly Detect DDoS/Worms

NARUS®

Take a walk on the Security Landscape

Backbone Market Evolution

NARUS®

PAST

Carriers treated data as "opaque"

-"Bits were bits"- they just passed traffic

Security was firewall based

- Endpoints were under attack, but not the network itself
- Fewer IP security risks (mostly viruses)

Security based on Firewalls

- Enough to protect the networks

PRESENT

Traditional carriers evolve

- Data outpaces circuit switched
- IP/MPLS Super-core emerges
- FM Convergence

CodeRed worm changed the threat landscape

- Security threats became commercially motivated
- Threats targeted network rather than endpoints
- Networks are larger and more open
- Attacks are highly distributed (DDoS)

Security based on IDS/IPS

- Appliances start to scale at very high-speed line-rate
- Enough to protect the network from DoS/DDoS IF close to the victim
- The appliance model is TOO expensive

FUTURE

Full IP Convergence: any network, any device

- IMS Super-access will emerge
- Carriers will monetize IP Services

New types of potential threats emerge

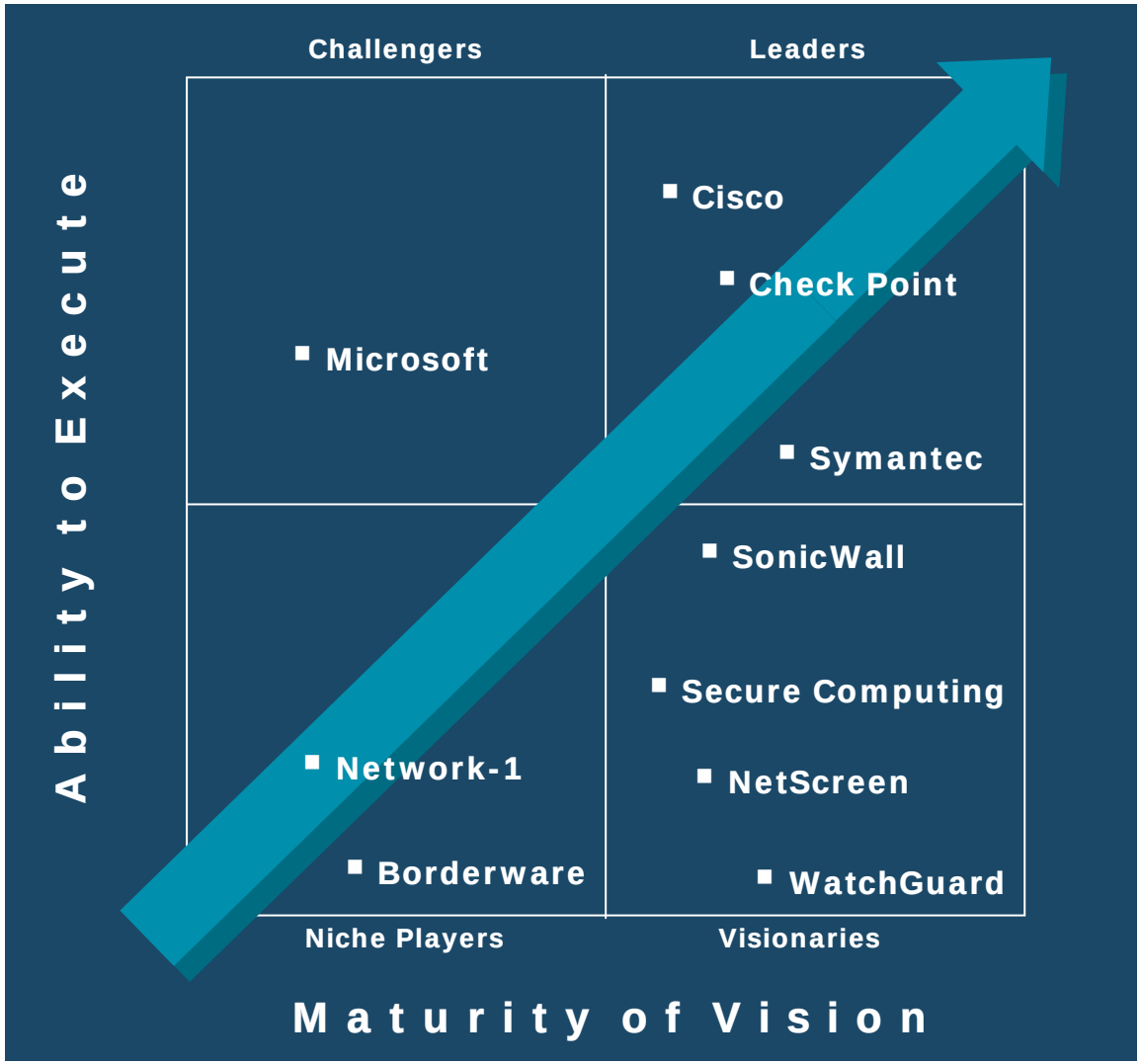
- Threads will target more and more IP services
- Attacks will be more and more distributed
- Polymorphic worms will emerge

Security based on IP Systems

- From Appliances to Systems
- Ability to collect information from any network element
- Ability to have fine-granularity visibility into traffic
- Ability to digest large amount of traffic

Market Snapshot 2001

NARUS®



Gartner Magic Quadrant for Firewalls update 2001

$2.4B Market

Single category

Backbone Market Evolution

NARUS®

PAST

Carriers treated data as "opaque"

-"Bits were bits"- they just passed traffic

Security was firewall based

- Endpoints were under attack, but not the network itself
- Fewer IP security risks (mostly viruses)

Security based on Firewalls

- Enough to protect the networks

PRESENT

Traditional carriers evolve

- Data outpaces circuit switched
- IP/MPLS Super-core emerges
- FM Convergence

CodeRed worm changed the threat landscape

- Security threats became commercially motivated
- Threats targeted network rather than endpoints
- Networks are larger and more open
- Attacks are highly distributed (DDoS)

Security based on IDS/IPS

- Appliances start to scale at very high-speed line-rate
- Enough to protect the network from DoS/DDoS IF close to the victim
- The appliance model is TOO expensive

FUTURE

Full IP Convergence: any network, any device

- IMS Super-access will emerge
- Carriers will monetize IP Services

New types of potential threats emerge

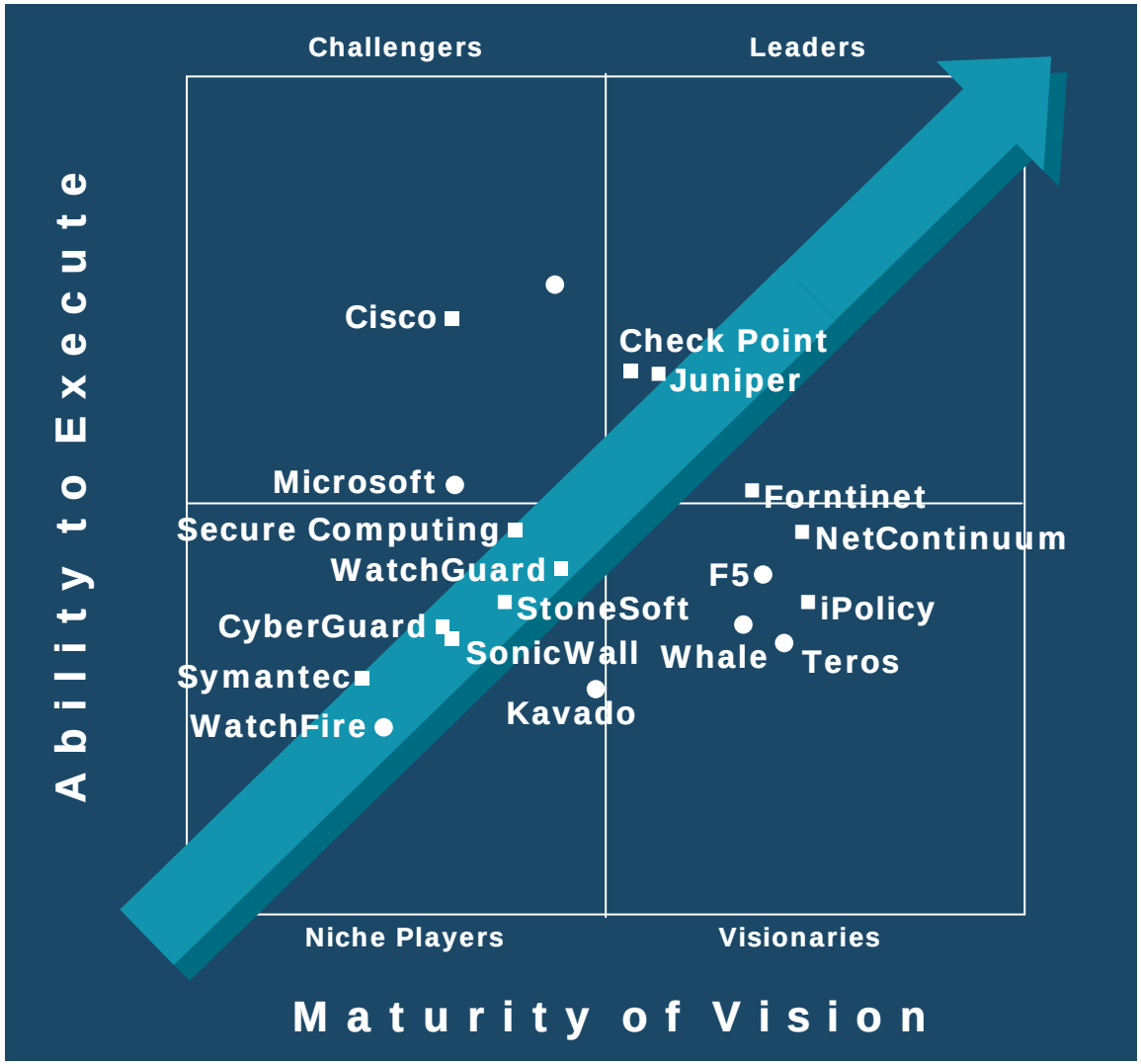
- Threads will target more and more IP services
- Attacks will be more and more distributed
- Polymorphic worms will emerge

Security based on IP Systems

- From Appliances to Systems
- Ability to collect information from any network element
- Ability to have fine-granularity visibility into traffic
- Ability to digest large amount of traffic

Market Snapshot 2004

NARUS®



Gartner Magic Quadrant for Firewalls update 2004

$8B

Much broader category

New set of leaders

Backbone Market Evolution

NARUS®

PAST

Carriers treated data as "opaque"

-"Bits were bits"- they just passed traffic

Security was firewall based

- Endpoints were under attack, but not the network itself
- Fewer IP security risks (mostly viruses)

Security based on Firewalls

- Enough to protect the networks

PRESENT

Traditional carriers evolve

- Data outpaces circuit switched
- IP/MPLS Super-core emerges
- FM Convergence

CodeRed worm changed the threat landscape

- Security threats became commercially motivated
- Threats targeted network rather than endpoints
- Networks are larger and more open
- Attacks are highly distributed (DDoS)

Security based on IDS/IPS

- Appliances start to scale at very high-speed line-rate
- Enough to protect the network from DoS/DDoS IF close to the victim
- The appliance model is TOO expensive

FUTURE

Full IP Convergence: any network, any device

- IMS Super-access will emerge
- Carriers will monetize IP Services

New types of potential threats emerge

- Threads will target more and more IP services
- Attacks will be more and more distributed
- Polymorphic worms will emerge

Security based on IP Systems

- From Appliances to Systems
- Ability to collect information from any network element
- Ability to have fine-granularity visibility into traffic
- Ability to digest large amount of traffic

A New Category Emerges

NARUS®

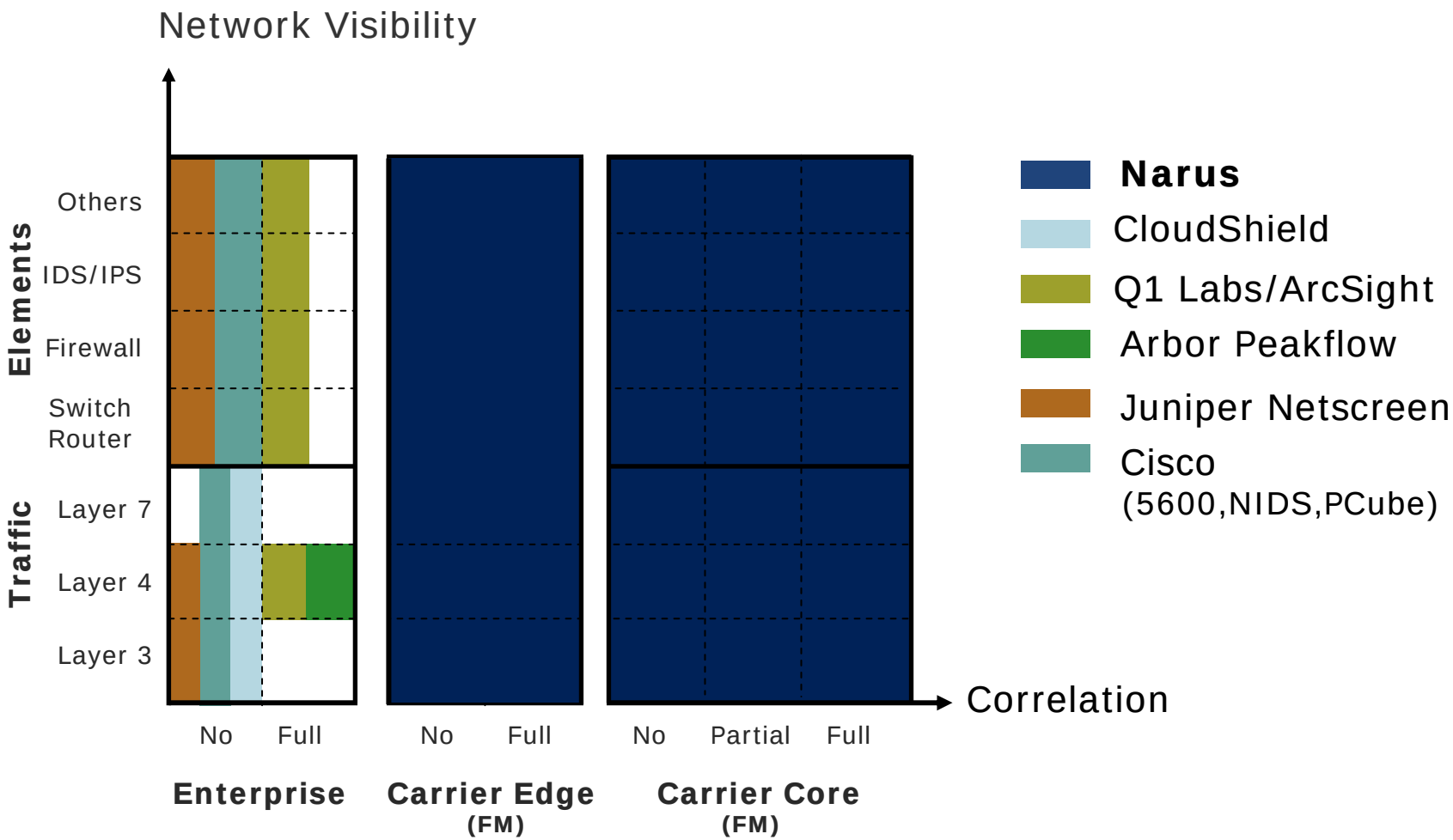
- Technology inflection
  - Rapidly expanding protocols and services (VOIP, Mobile-IP, IMS)
  - Inflections demand next generation performance
    - Today's architectures provide limited scaling
    - *Services require* capture layer 3,4&7 data at OC48 and OC192 speeds
- Increasing Demand over time
- Few entrants, very little competition
- Technology inflection
  + market acceptance + little competition
  = **a new category**

Security Defense-Shield: Requirements

NARUS®

- Full Control of the Network requires a Unified Vision of the Network
  - Point Solutions can be ineffective for distributed attacks
- IP Traffic Granularity
  - Centralized Normalization and Correlation of multiple source of data
- Cutting-edge Algorithms
  - Adaptive
  - Efficient
  - Scalable
  - High-performance

Let's take a snapshot at the market

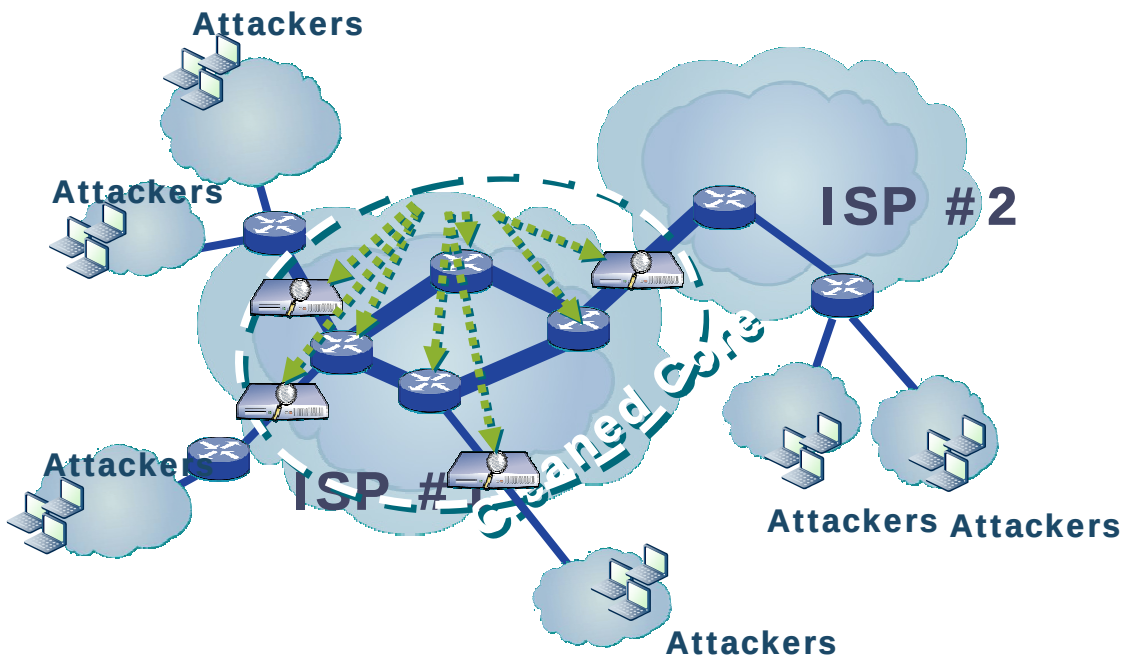


NARUS®

Bounce the Attacks at the Edge: Defense-Shield

Example:

DDoS and Worms



“Attacking a System” is equivalent to “Perturbing its Equilibrium-Point”

- Each Element in the Universe obeys to Physical Laws
- Any perturbation applied to any stable system breaks the system’s equilibrium
- Internet is a Physical System that obeys to Physical Laws
- Internet Traffic is structured in some ways (invariant component) and very random in others (variant component)
  - Users are methodic and unpredictable at the same time
- Threads represents a “deterministic” actions that affect the equilibrium of the system:
  - Strong Temporal Coordination across Attackers (DDoS)
  - Abnormal large host-population contacted by Infected Host (Worm)

Detect a perturbation of equilibrium-point

NARUS®

- Information Entropy:
  - DDoS, Worms, etc, disrupt over time the "*structure*" and "*randomness*" of key traffic features
  - Information Entropy is a powerful operator to detect a change in traffic distribution on-fly:

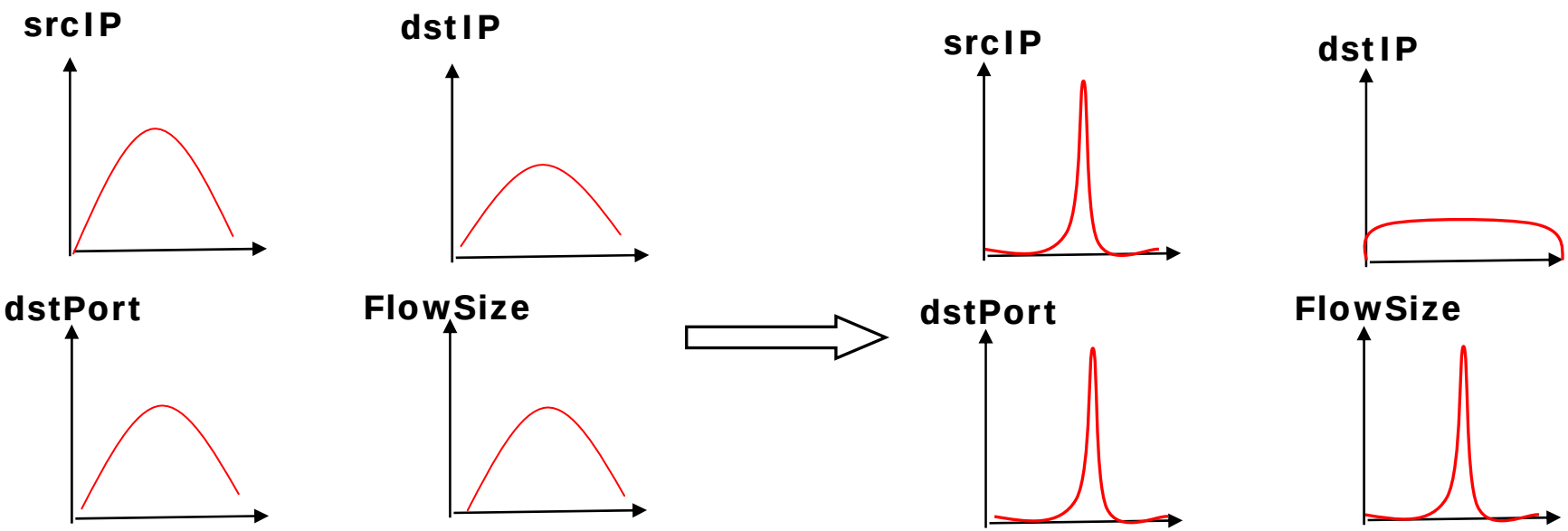
$$H_i^X = -\sum_{p \in P_i^X} p \log_2 p$$

  - Skew-distribution: low-entropy / Flat-distribution: high-entropy
  - Information Entropy can be well approximated by well-known data mining algorithms
    - Requires a few CPU cycles
    - Requires bounded memory
- DDoS & Worms disrupt the key-feature distributions

Change of distributions when under attack, example Worm

NARUS®

- Key Traffic Features: <SrcIP>, <srcPort>, <dstIP>, <dstPort>, <FlowSize>:
  - A few srcIP -> many dstIP
  - Specific Application Vulnerability -> ONE dstPort (it can be different)
  - Small flows become dominant



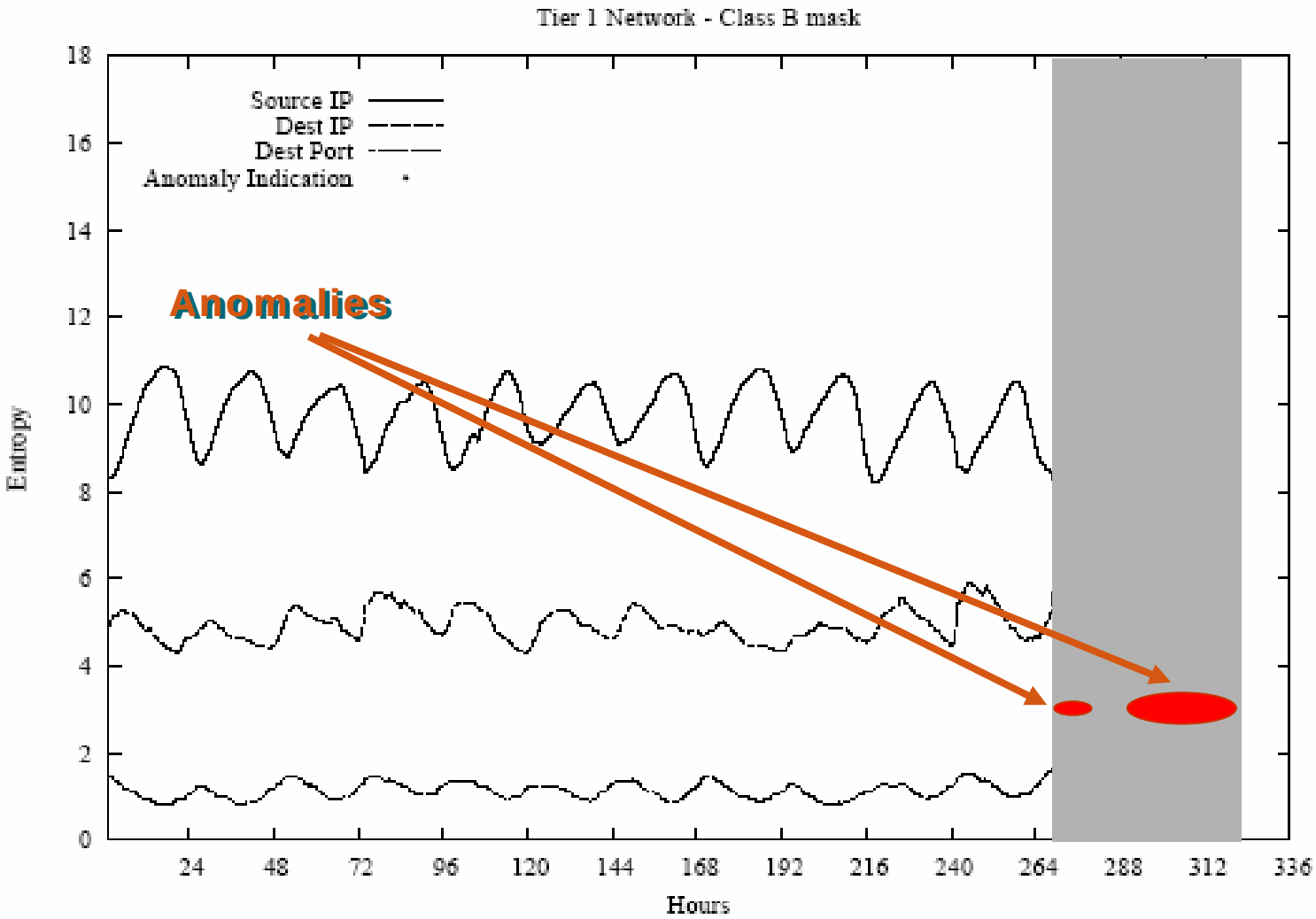
High-Level Sketch of the Algorithm: example, Worms

NARUS®

- Step #1: Based on Layer-4 information
  - Extract the marginal distributions of five key features:
    - <SrcIP>, <DstIP>, <SrcPort>, <DstPort>, <FlowSize>
  - Compute *Entropy* for the above marginal distributions
  - Mark malicious flows as “suspicious”
    - Hosts for which a deviation of the GlobalMetric is observed
  - Generate a flow-filter mask using key features for which a drop in the entropy is observed
    - Example, <SrcIP,DstPort,FlowSize>
- Step #2: Based on Layer-7 information
  - Apply flow-filter mask to isolate and deeply-analyze ONLY “suspicious” flows
  - Extract Worm-Signatures ONLY for “suspicious” hosts
    - Rabin, Longest-Common-SubString, Longest-SubSequenceString, etc

Algorithm in action: Tier-1 Wireless Network

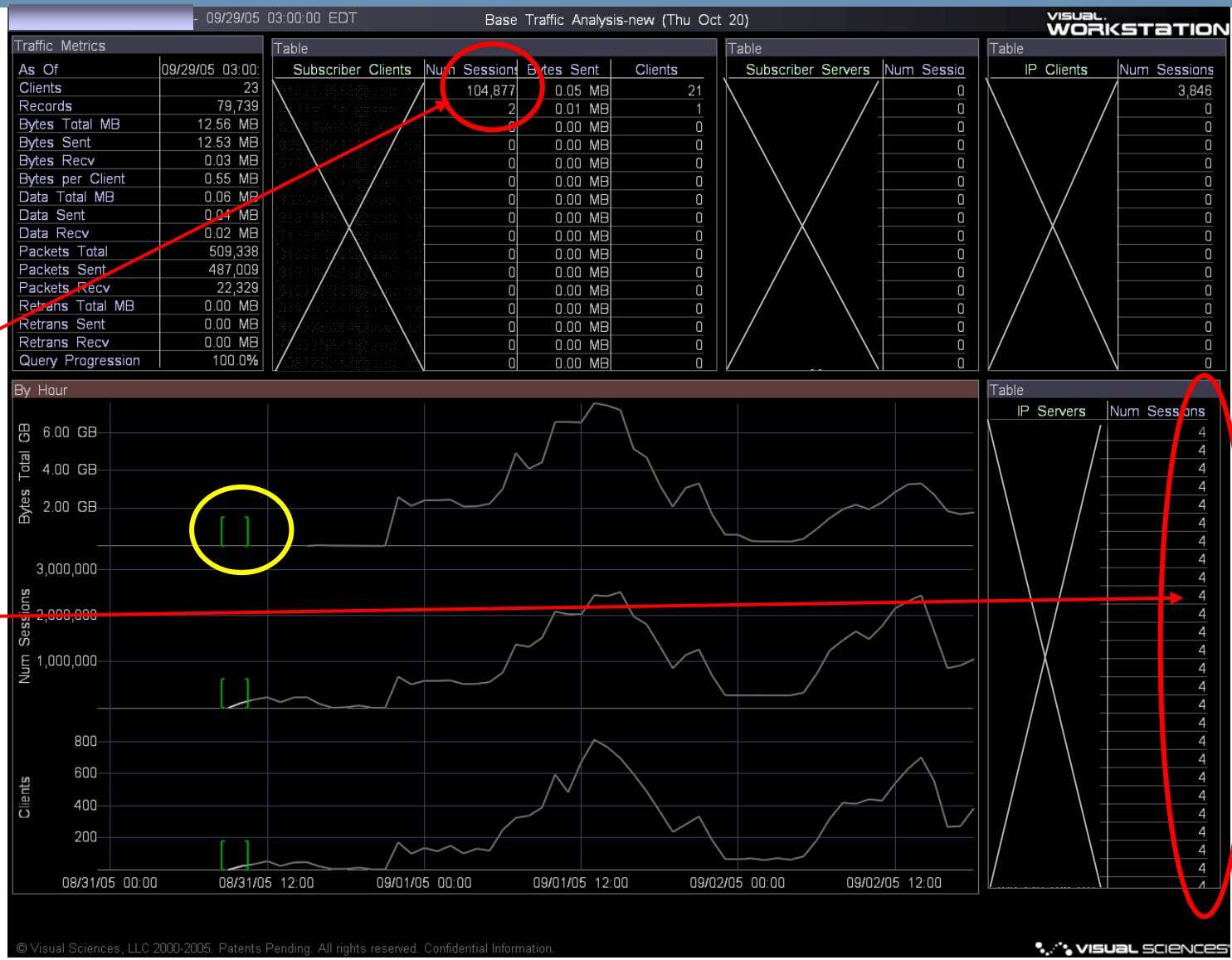
NARUS®



Results from Tier-1 Network (Sasser): TCP Port 445 – The 1st Hour

NARUS®

- **The first uptick in TCP Port 445 traffic happened on 8/31/05 between 9:00 to 10:00 AM**
- **This NarusView drilldown on the first hour revealed that TCP Port 445 traffic was generated almost totally by one Subscriber Client X**
- **During the first hour, a distinctly "deterministic" number of sessions (e.g., 4) were set up by subscriber X to numerous IP servers, symptomatic of worm propagation**



Results from Tier-1 Network (Sasser): TCP Port 445 – The 13th Hour

NARUS®

- **The second significant uptick in TCP Port 445 traffic happened 12 hours later, from 9:00 to 10:00 PM on 8/31/05**
- **This NarusView drilldown on the 13th hour revealed that the number of Subscriber Clients generating TCP Port 445 traffic had grown to 6**
- **On the 13th hour, distinctly "deterministic" number of sessions (e.g., 4, 14) were set up to numerous IP and Subscriber servers, again symptomatic of worm propagation**

Results from Tier-1 Network (Sasser): TCP Port 445– The 21st and 22nd Hours

NARUS®

- **The third significant uptick in TCP Port 445 traffic happened 7 hours later, from 5:00 to 7:00 AM on 9/1/05**
- **This NarusView drilldown on the 21st and 22nd hours revealed that the list of Subscriber Clients generating TCP Port 445 traffic had grown further to 12**
- **During the 21st and 22nd hours, distinctly "deterministic" number of sessions continued to be set up to numerous IP and Subscriber servers, symptomatic of worm propagation**

NARUS®

Thanks

Thanks

QUESTIONS?

Thanks

Thanks

Thanks

Thanks