



Managing & Controlling Application
Performance

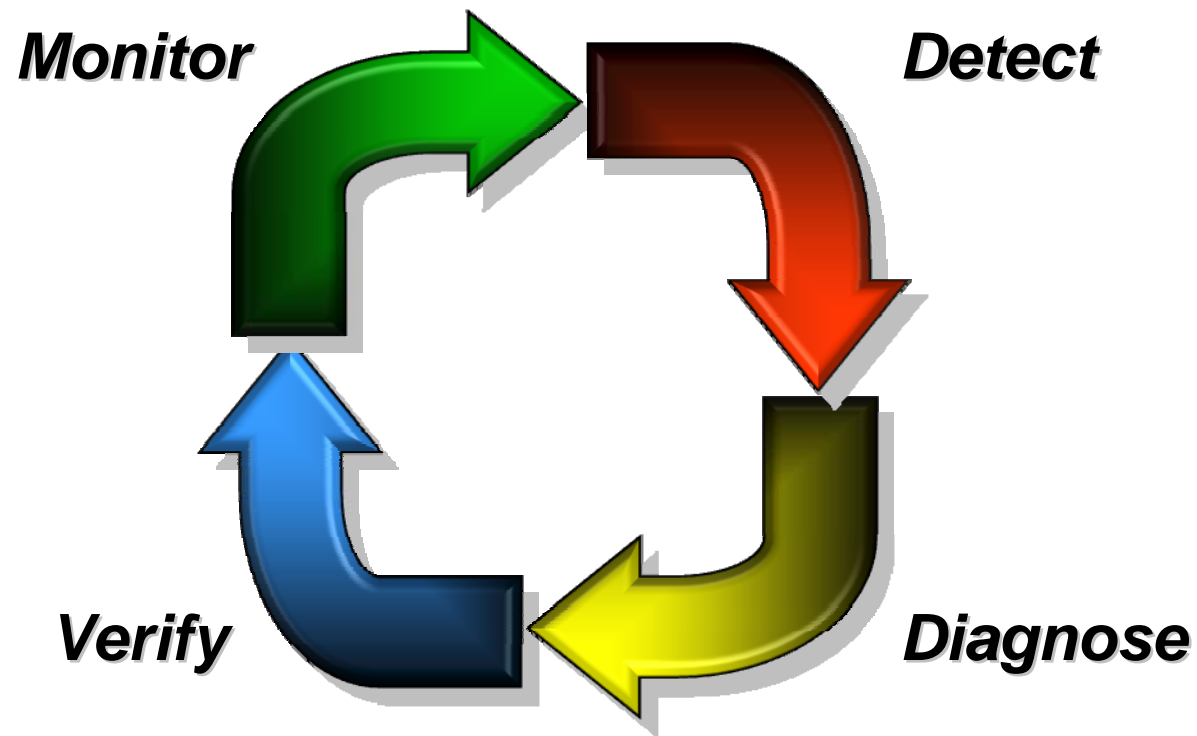
Dealing With Degradations

Jim Frey
VP Marketing
www.netscout.com

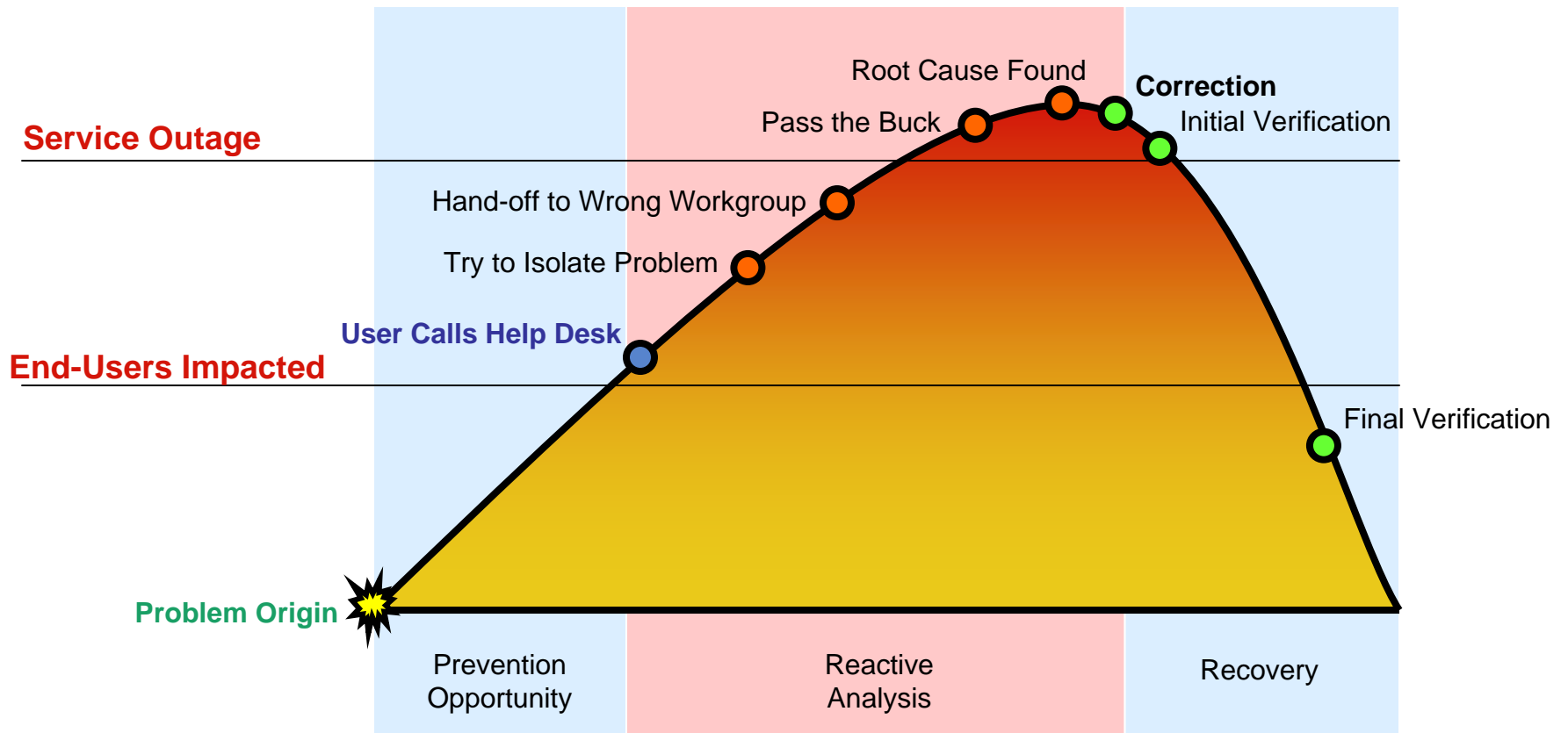
Agenda

- The Performance Problem Lifecycle
- Detecting Degradations
- Diagnostic Velocity
- Case Examples

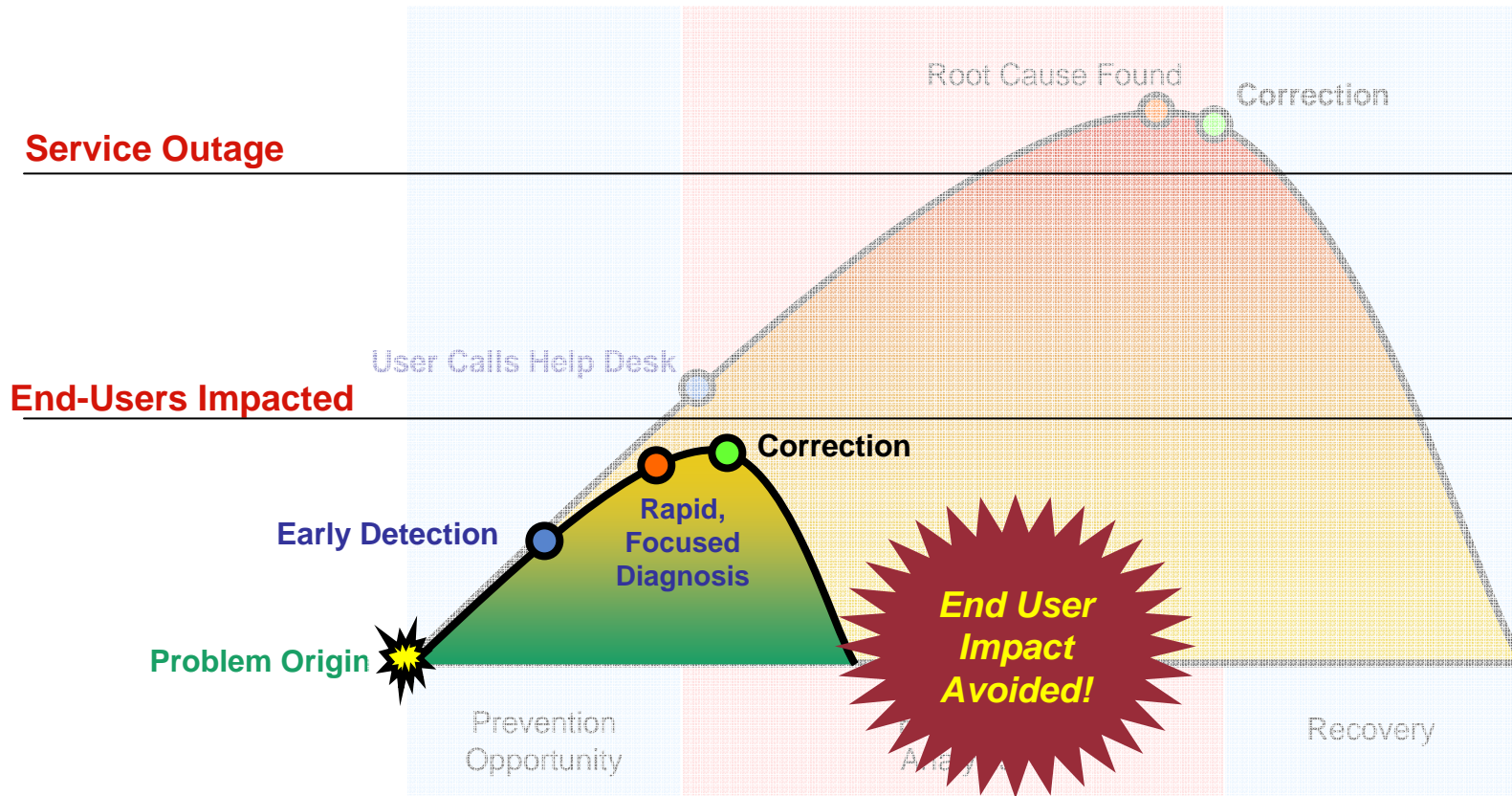
Performance Problem Lifecycle



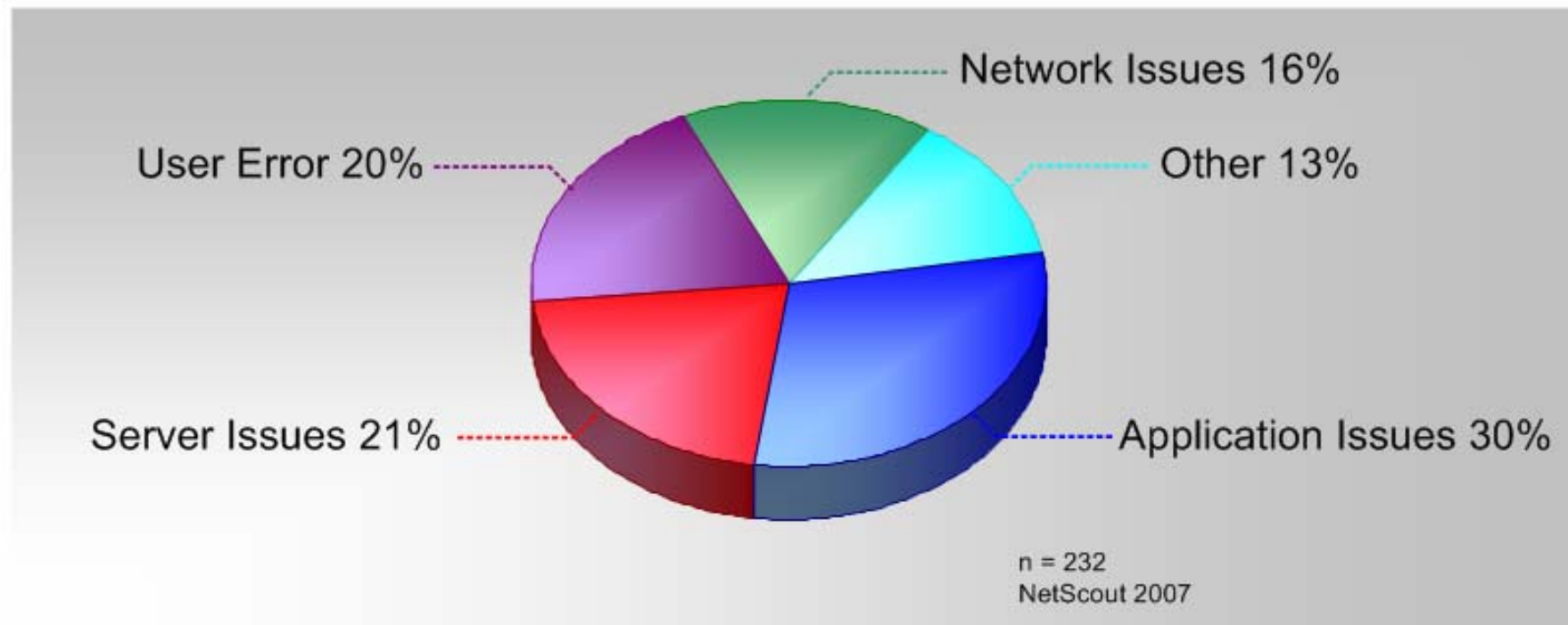
Typical Lifecycle Scenario



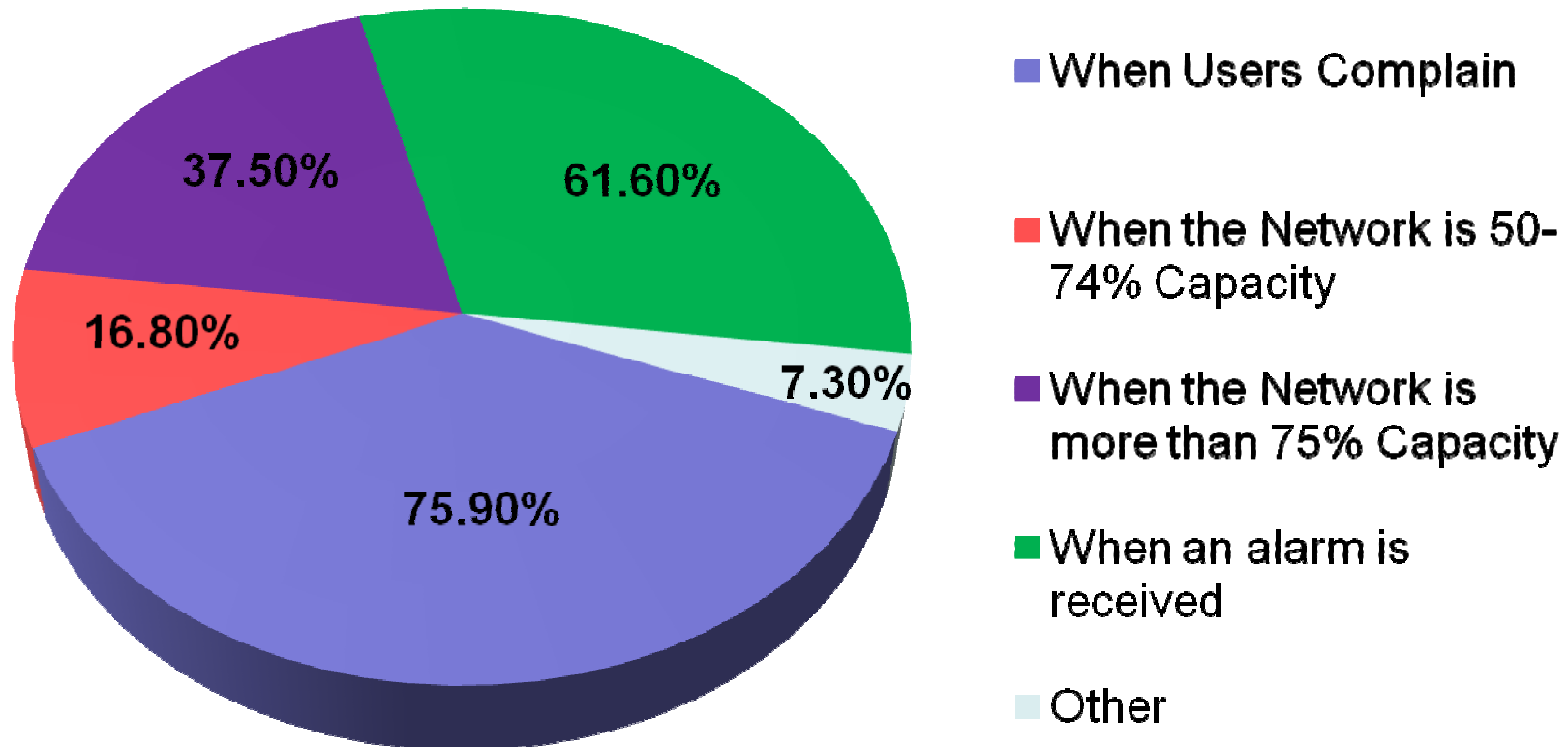
The Ideal Case



What is the Source of Performance Issues?



Who Finds Performance Problems?

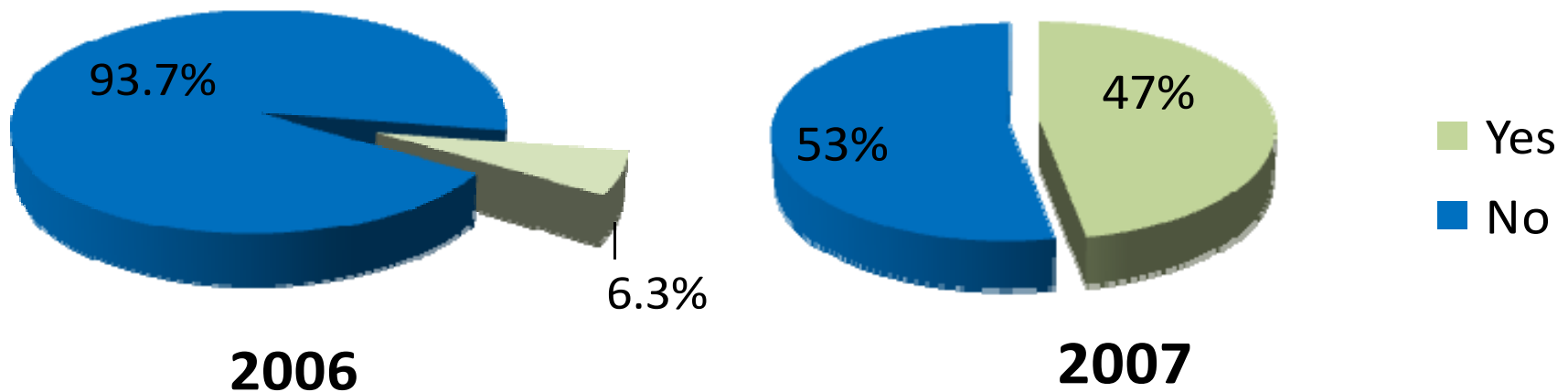


Source:
NetScout Systems Survey
March 2007
N = 232

Note: Respondents may have chosen more than one answer

Personal Goals tied to Fast Restoration

Do you Have any MBOs Related to MTTR?



Detection Priorities

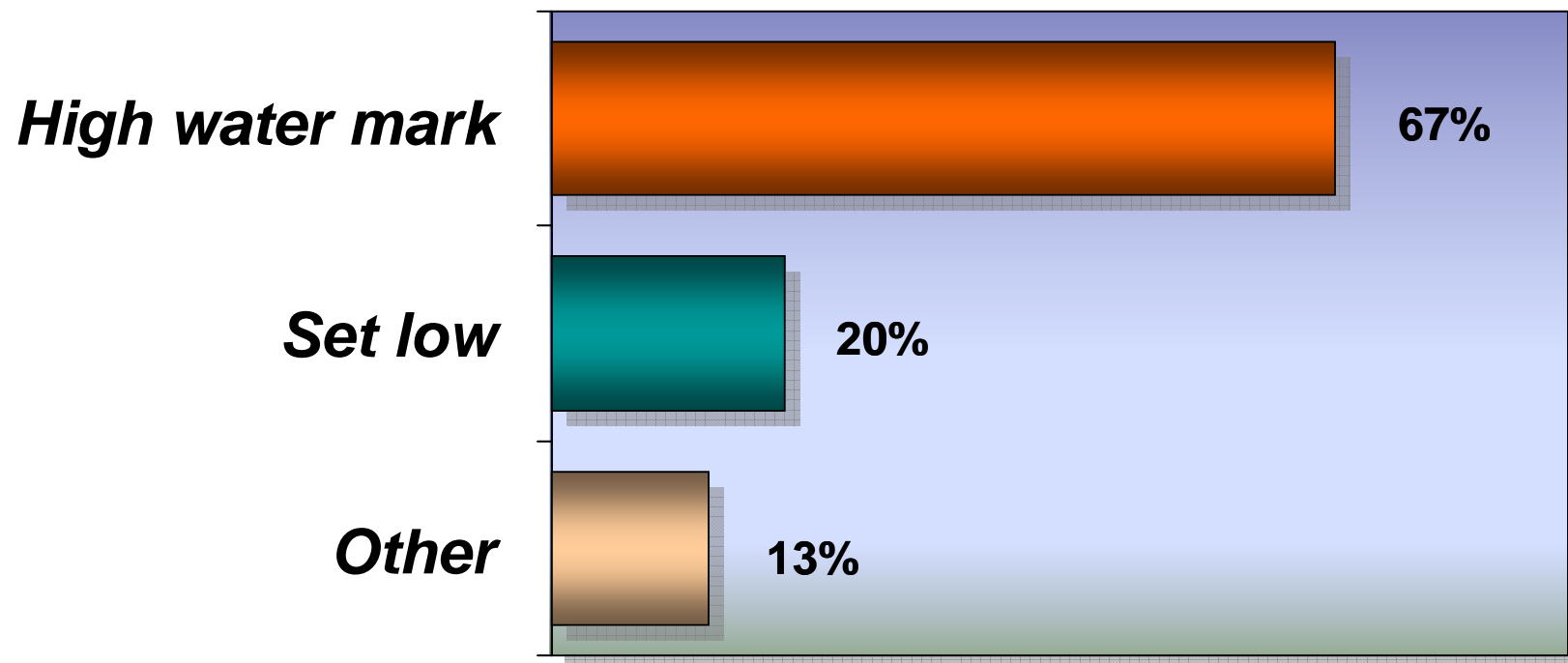
Reactive/Immediate Issue

- Timeliness
- Accuracy

Proactive/Potential Issue

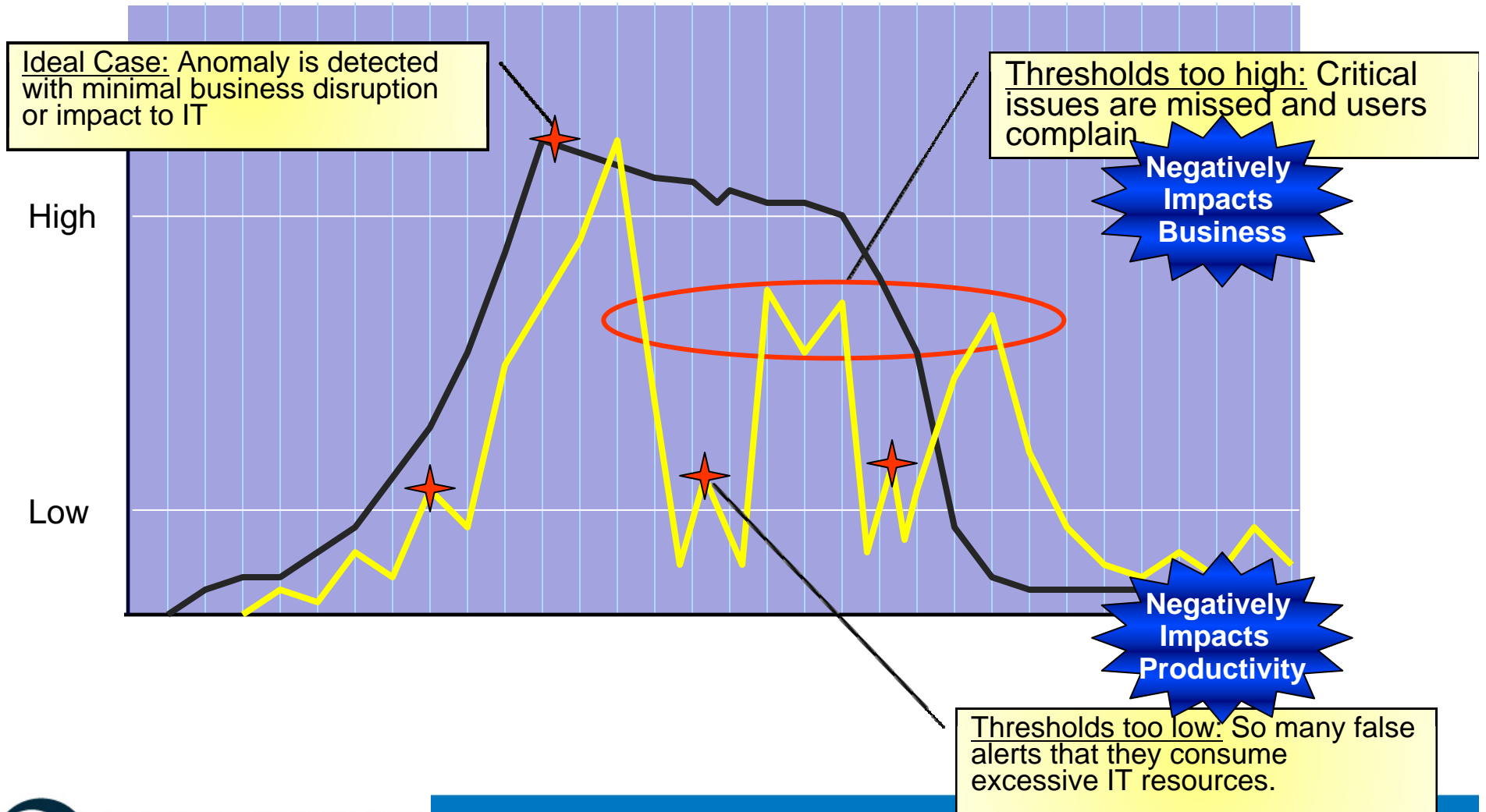
- Early (Enough)
- Relevance

Current Common Practices: Setting Performance Thresholds



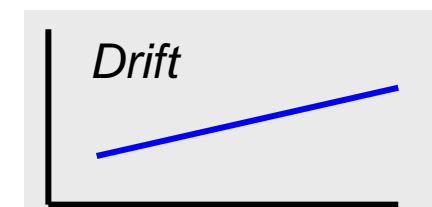
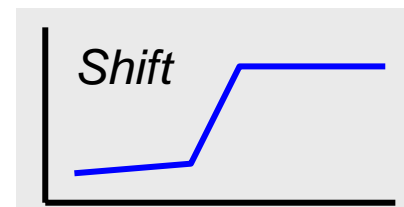
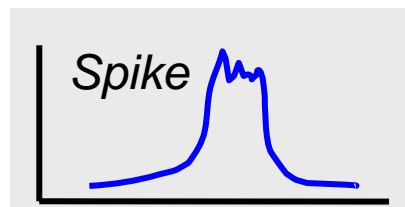
Source: Ashton Metzler & Assoc., 2006
N = 231

The Problem with Static Thresholds...

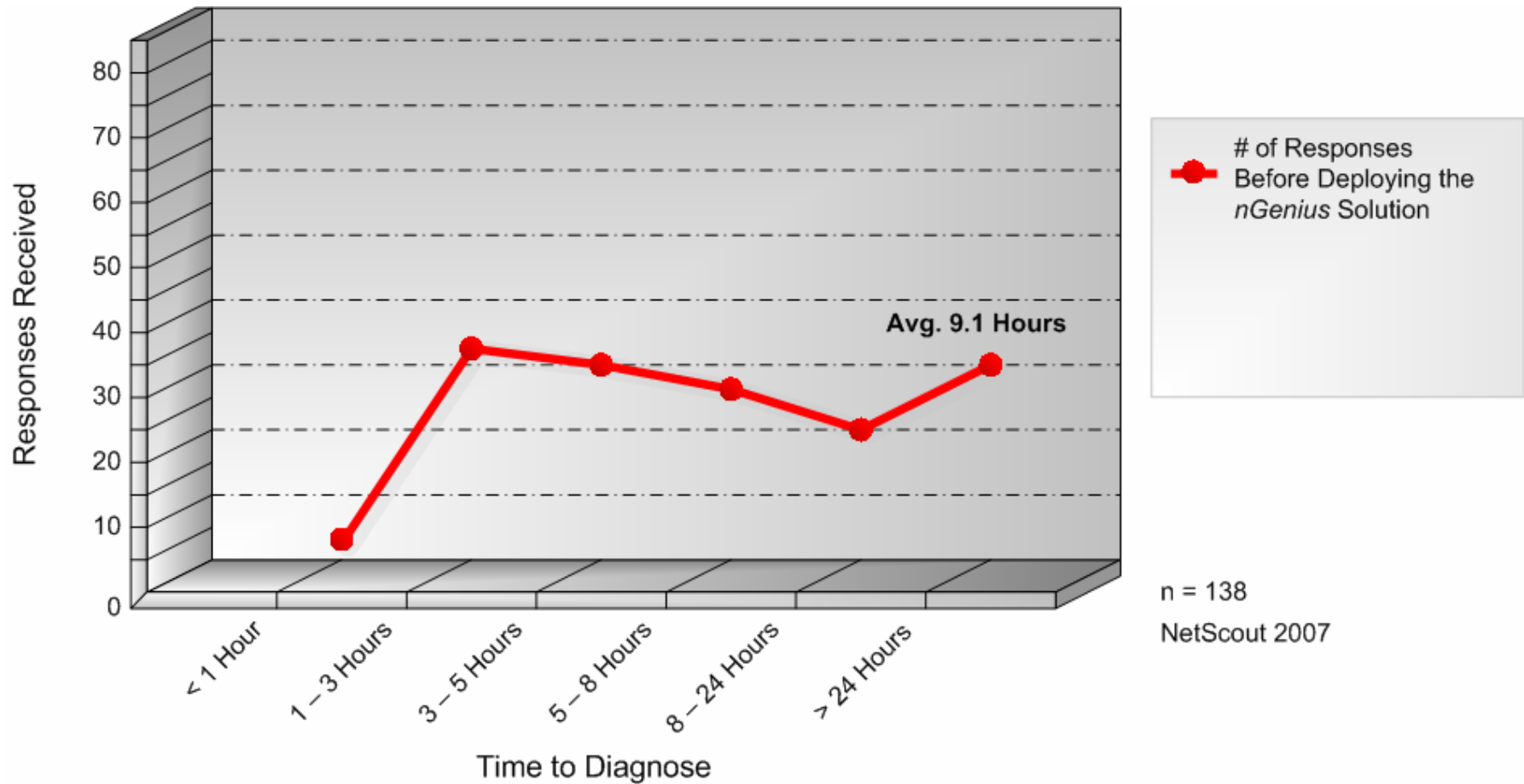


A Better Alternative: Intelligent, Automated Analytics

- Learns patterns of usage
 - Constantly updated statistical model
 - Applied at physical, virtual, & QoS class levels
- Automatically detects anomalous behavior
 - Recognizes relevant departures from normal
 - Progressive Analytics™ accelerates diagnosis and correlation
- Delivers “Threshold-less” alarm management, reducing
 - Time spent configuring alarms
 - # of false alarms and # of missed alarms
- Categories of Problems:



How Long Does Diagnosis Take?

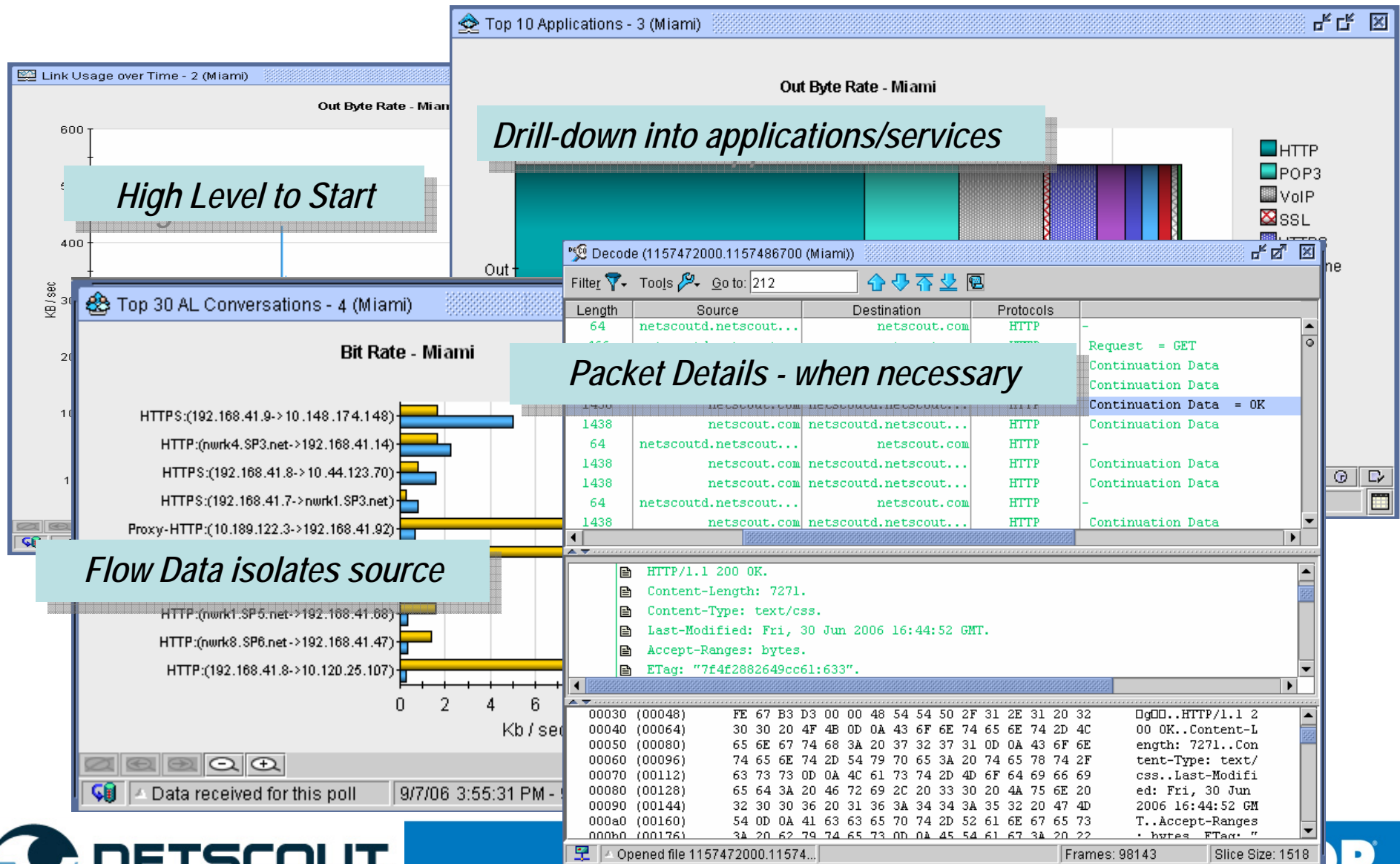


Achieving Diagnostic Velocity

Requirements

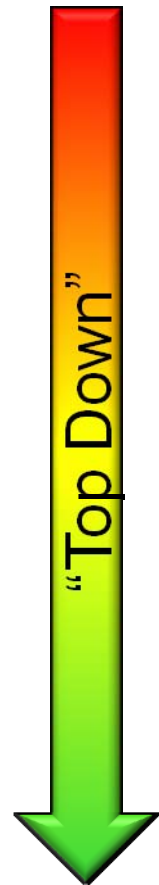
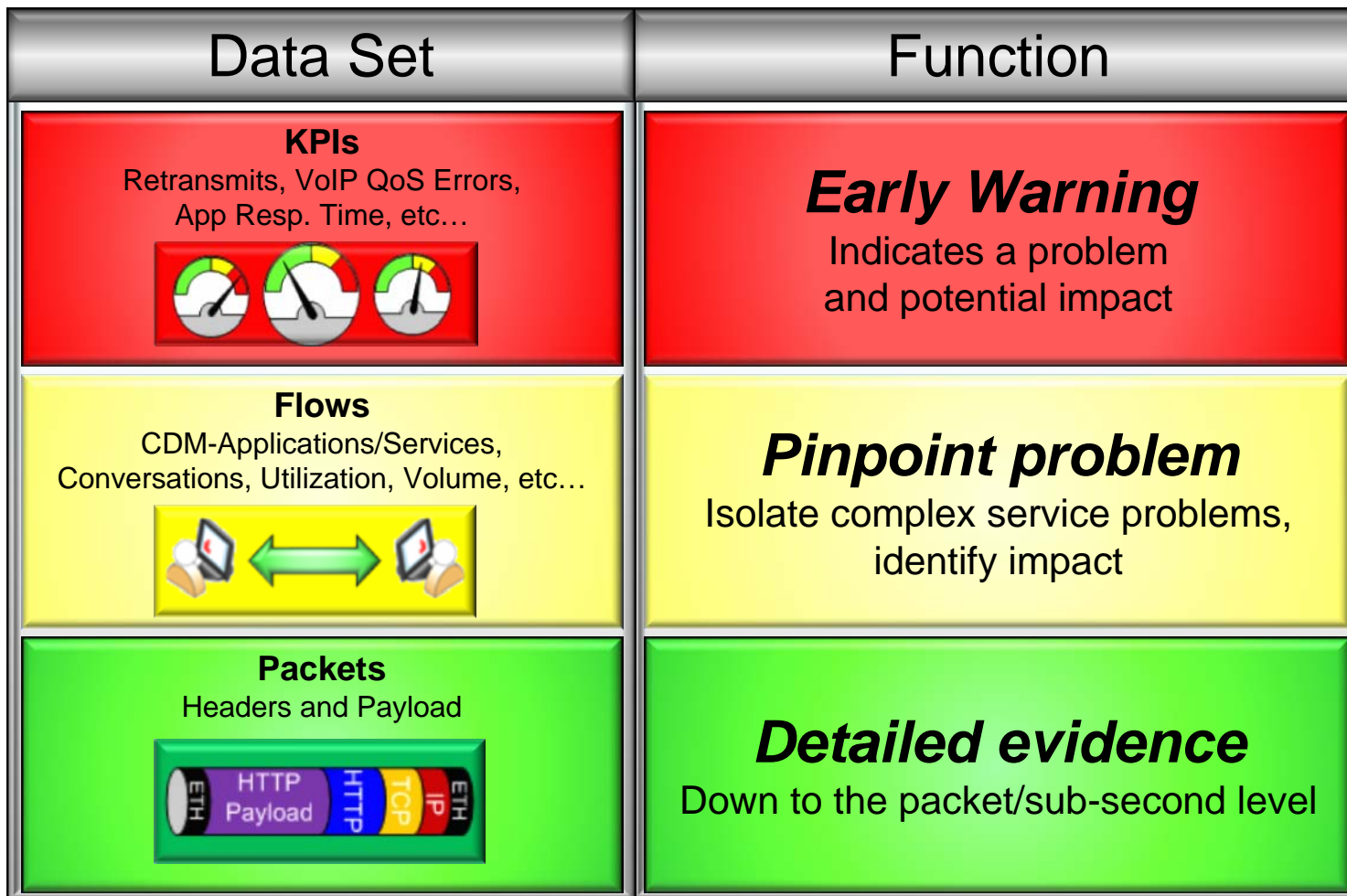
- Breadth of Data
- Depth of Data
- Workflow Efficiency
- Ease of Collaboration

Data Breadth & Depth

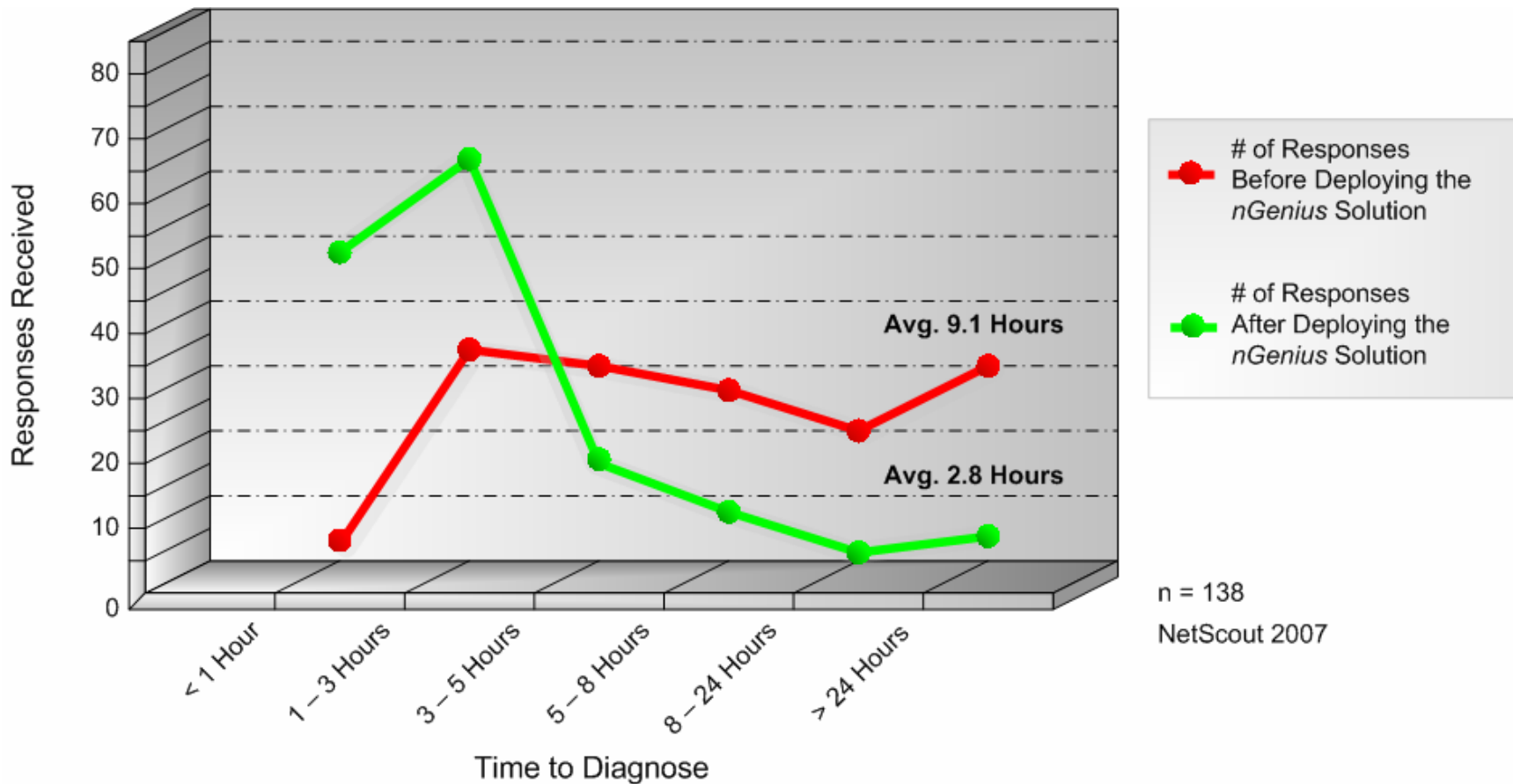


NetScout's Unique Approach

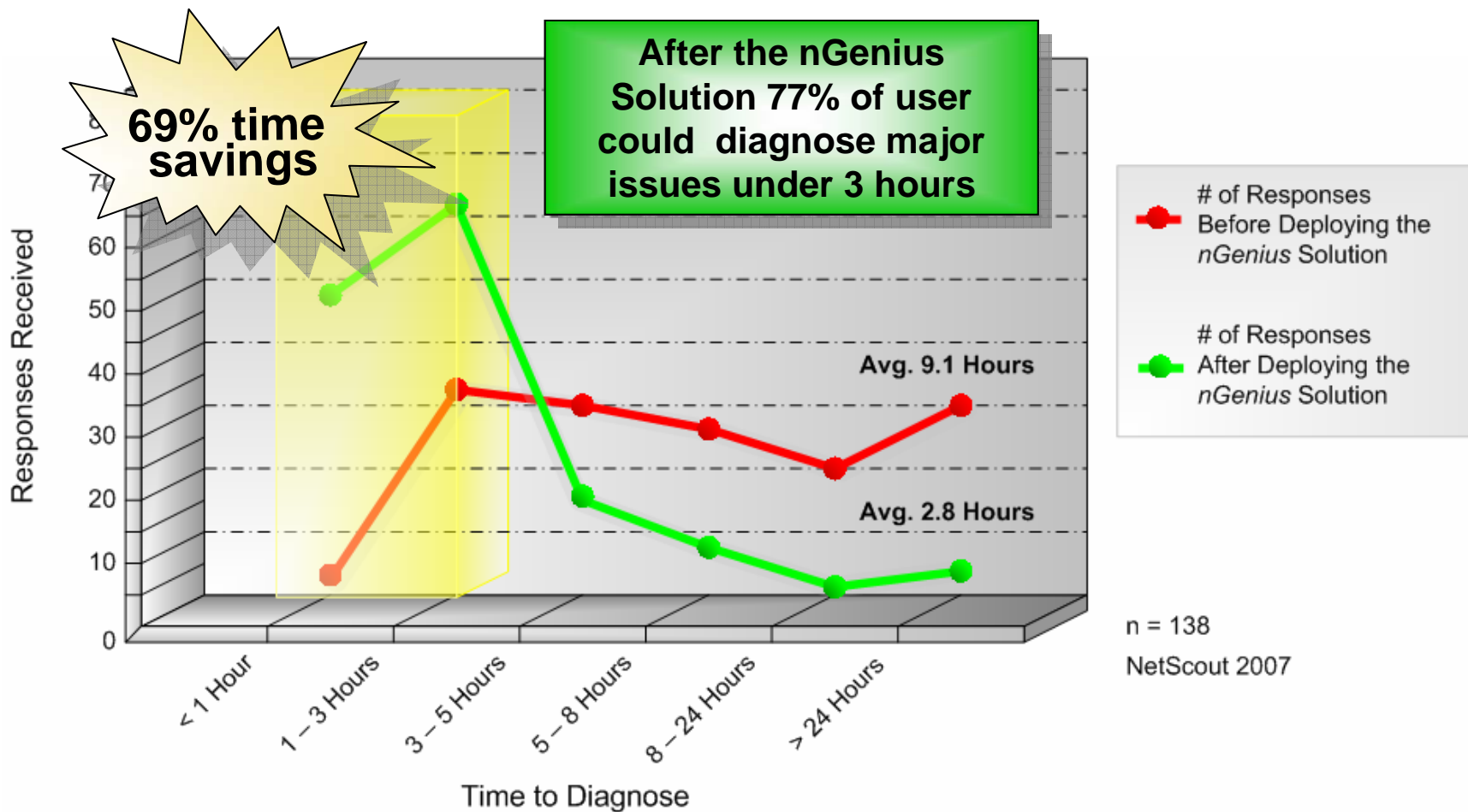
Three-Tier Data Architecture for Rapid Top-Down Workflow



The *nGenius* Solution Difference



The *nGenius* Solution Difference



Case Example #1

Nation-wide Insurance Carrier

Problem

- Access to corporate network resources degrading

Method of Detection

- *nGenius* Analytics alarm identifying high LDAP utilization

Diagnosis

- *nGenius* Performance Manager drill-down:
 1. Application & conversation flow analysis between servers
 2. Packet decodes on recorded packets revealed

Source/Correction

- Two servers unsuccessfully attempting to re-sync
- Once both reset, performance of the LDAP servers and overall traffic volume returned to acceptable levels

KPI-to-Flow-to-Packet Troubleshooting Example

The screenshot displays the NetScout Administrator interface. The main window shows an alert for 'Decode (LDAP.pcap (HQ_NY:if4))' with a severity of Medium. The interface includes several panels:

- Alert Details:** Shows severity (Medium), interface (HQ_DFW:if4), IP address (192.168.99.151), and a description: 'Increased utilization in a modern...'. It also features a graph titled 'Application Usage over...' and 'In Utilization - 15 min'.
- Decode (LDAP.pcap (HQ_NY:if4)):** A packet analysis window showing a table of frames. Frame 29 is highlighted, showing details for an LDAP packet with a 'Decode Status : BAD CHECKS' and a 'Checksum should be : 0xA...'. A red circle highlights the 'Checksum should be' field.
- Bounce Chart - 2 (LDAP.pcap) 192.168.50.64<->192.168.61.201:** A chart showing the timing of packets between two servers. The chart includes a table with columns for Frame, Source, Destination, Delta Time (sec), and Relative Time. The table shows 13 frames with significant delays between frames 1 and 2, and between frames 11 and 12.

Bounce chart from decode analysis shows 2 servers with problem syncing between each other.

Frame	Source-192.168.50.64:964	Destination-192.168.61.201:964	Delta Time (sec)	Relative Time
1	IP Total Len = 278 Identification = 2111 Message_Length=244 SearchRequest ID=32914 Base_Object=[0 byte(s) of data]		0.000	0 us
2	IP Total Len = 278 Identification = 5510		909.444	15.1574 min
3	IP Total Len = 278 Identification = 14207		900.046	30.158167 ...
4	IP Total Len = 235 Identification = 19170		824.792	43.9047 min
5	IP Total Len = 278 Identification = 19328		65.786	45.001133 ...
6	IP Total Len = 278 Identification = 22779		909.513	1.002661 hr
7	IP Total Len = 235 Identification = 56034		5331.603	2.483662 hr
11	IP Total Len = 278 Identification = 19627		3609.708	4.002824 hr
12	IP Total Len = 235 Identification = 20520		328.607	4.094104 hr
13	IP Total Len = 235 Identification = 20523		4.430	4.095334 hr

Case Example #2

Major Metropolitan Hospital

Problem

- VoIP Phones Deregistering

Method of Detection

- *Massive end user unhappiness*

Diagnosis

- *nGenius* Performance Manager
 - QoS Group View
 - VoIP Traffic Details

Source

- Asynchronous QoS assignments

Case Example #3

Global Manufacturing Company

Problem

- Application time-outs

Method of Detection

- End user complaints

Diagnosis

- *nGenius* Performance Manager with *nGenius* AFMon
 - Applications over Time View
 - Host & Conversations Details Table
 - Packet decodes on recorded packets

Source

- Found switch that was dropping packets when site swamped with broadcast traffic

Summary

- Users typically find performance issues before you do
- It *is* possible to be more proactive
- Take a step back and look at your infrastructure from the application's viewpoint
- The answers are in the management data – expect your vendors to help!

NetScout Systems
Booth 628