

Network Behavior Analysis (NBA) Systems: The New Foundation of Defense-in-Depth

Charles Kaplan
Chief Security Strategist, Mazu Networks

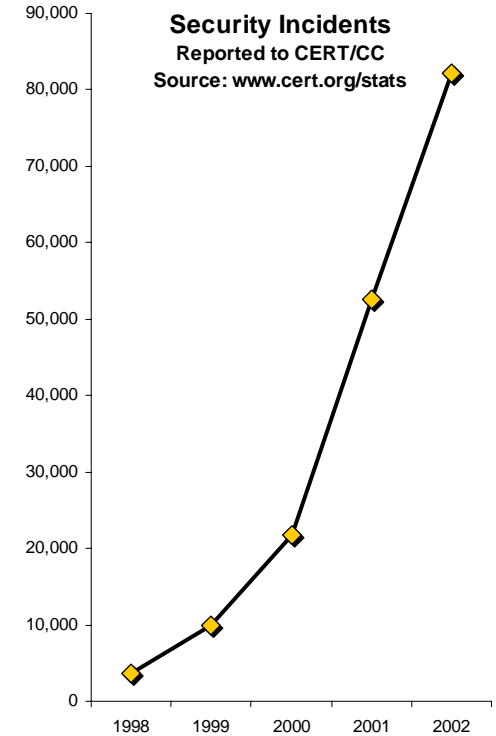
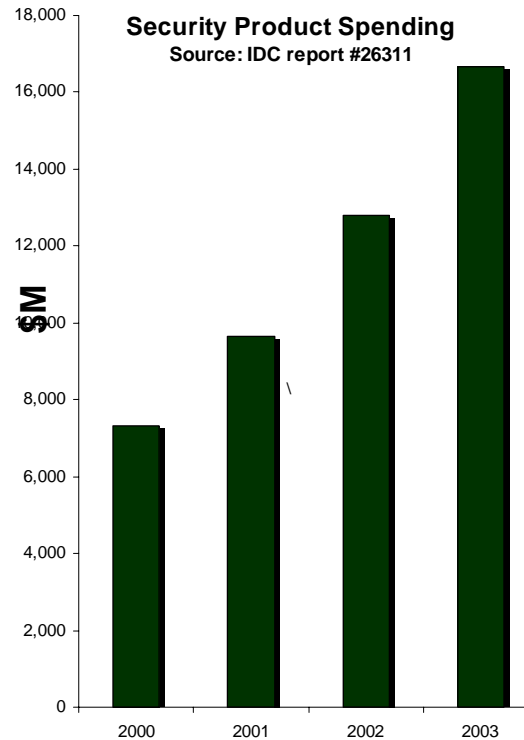
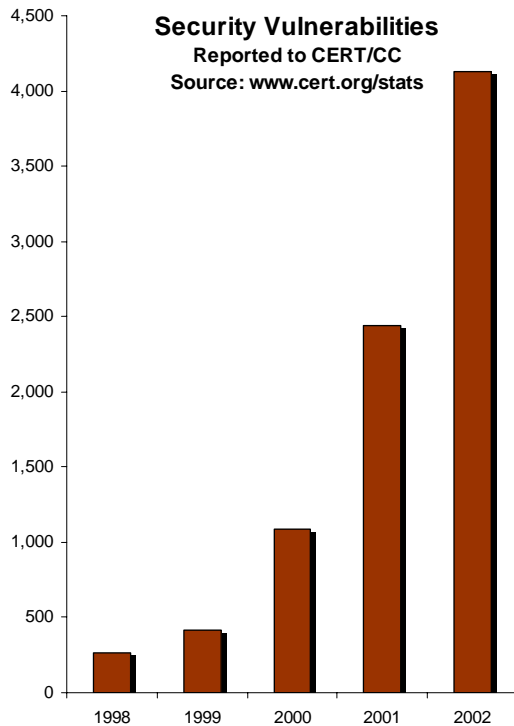
ckaplan@mazunetworks.com

INTEROP[®]
MAKES YOU
SUCCEED

Introduction

- Who am I?
- Why am I here?
- What is today's takeaway?

Today's Strategies Aren't Working



Record Vulnerabilities

Record Spending **AND** Record Incidents

**Sources: International Data Corporation and CERT (cert.org)*

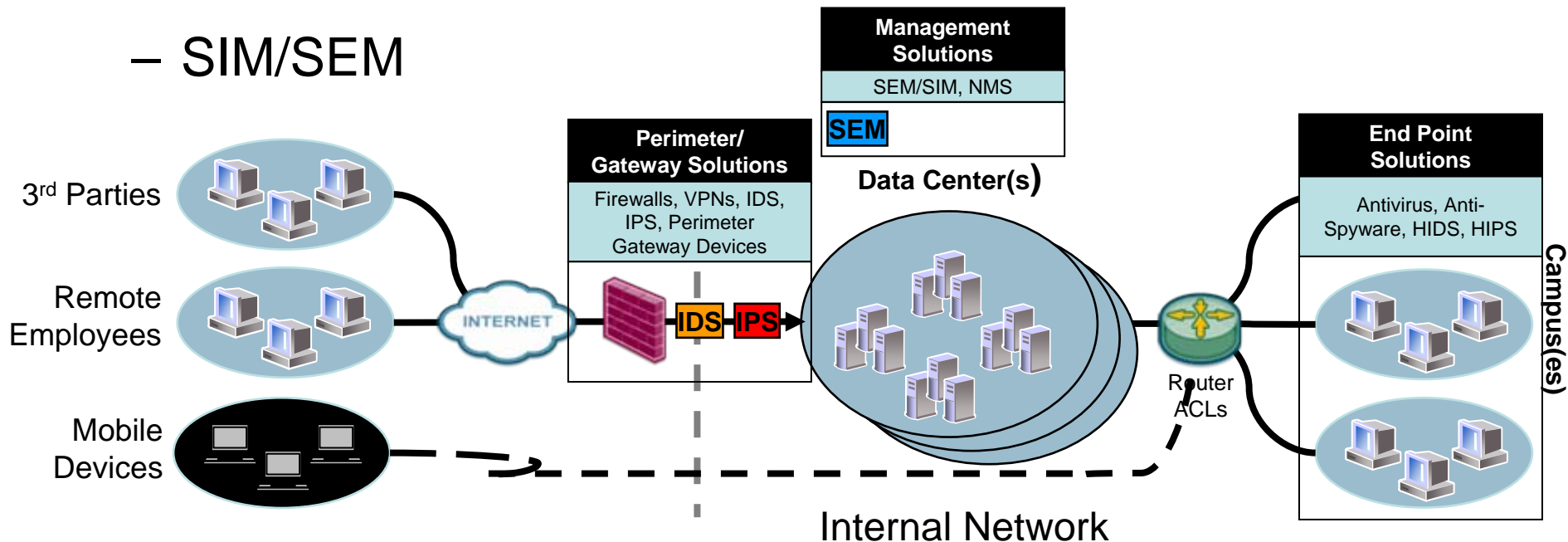
Takeaways from Enterprise Strategy Group

- External threats and protections are well understood
 - Costly to deploy and operate, standardized in approach
- Internal threats are difficult to quantify and understand
 - Not well protected against
- Conventional technologies are not sufficient to reliably detect that which we cannot quantify

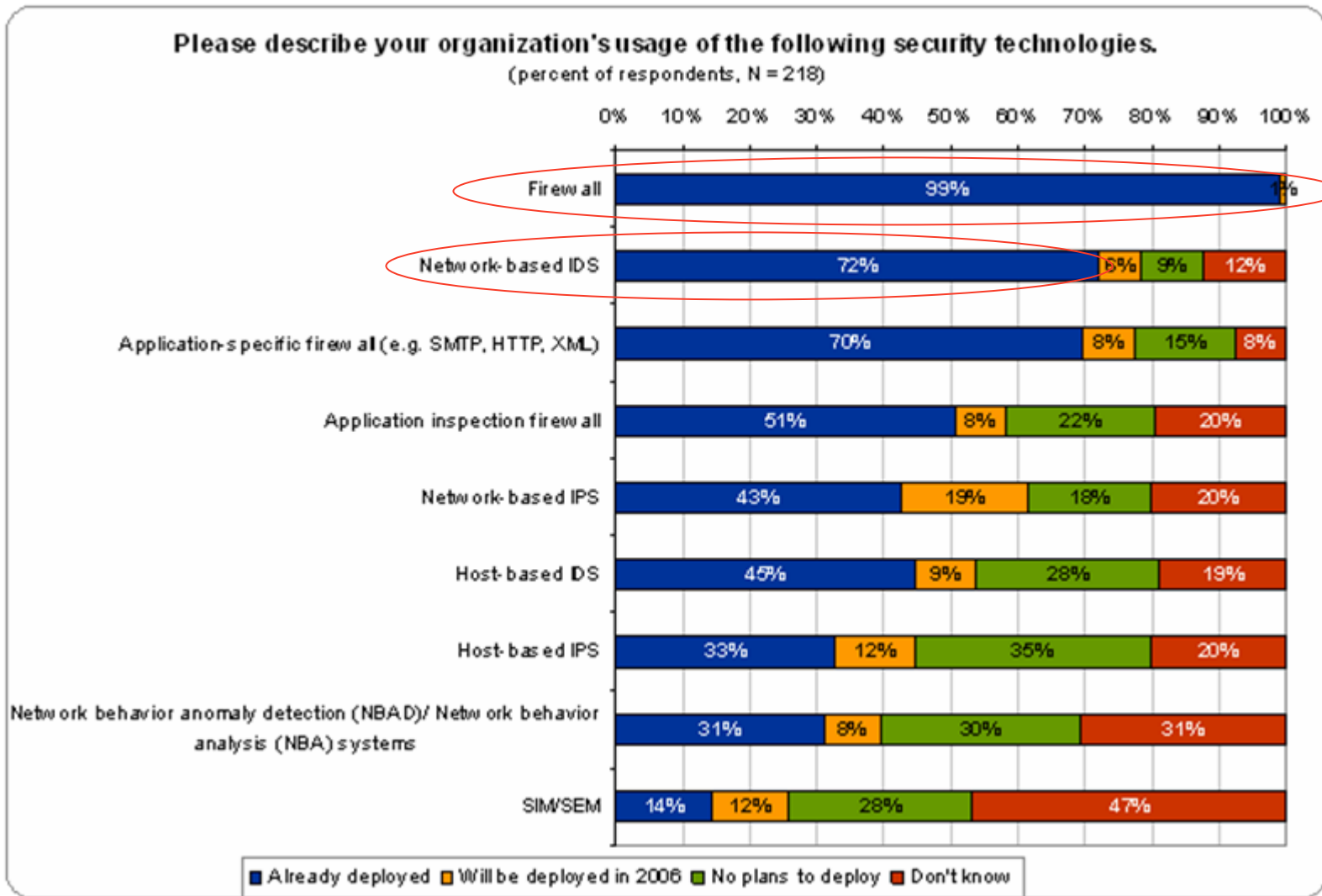
Status Quo is not adequate in the face of an increasing threat landscape.

Do We All Understand Perimeter Security?

- Who in the audience is not familiar with the following technologies?
 - Firewalls
 - IDS & IPS
 - VPNs
 - SIM/SEM



Current Security Defenses



Source: Enterprise Strategy Group 2006 Internal Threat Report

Recent Attack Vectors

- **System theft/loss**
 - Fidelity Investments (March)
 - Health Care America (August)
 - Husband and wife I used to work with at VeriSign
 - Veterans Affairs (May)
 - Sovereign Bank (August)
- **BBery proxy** - Discussed at Black Hat this summer
- **Spear Phishing with boutique viruses**
- **Corrupt employees** - Coca-Cola admin tries to sell info to Pepsi-Cola
- **Bad business practices** - Card Systems
- **The average Joe employee** - Leaves his old job for new and copies the entire CRM DB, or CVS repository
- **MS06-040**

How Protected Are You?

- How many of you have controls in place to address these kinds of threats?
- Who here in the audience believes that current 'best practices' will detect these attacks?
- Are these technology or policy threats?
- Lets take a look at our conventional Defense-in-Depth strategy today ...

Defense-in-Depth (DiD)

- A term coined by the Department of Defense
- A philosophy on complete system integrity
- Placement of defenses such that the compromise of one mechanism doesn't make one defenseless

InfoSEC is a world of system mis-configurations, software bugs, disgruntled employees, and overloaded system administrators.

DiD – a Practical Example

Your corner bank



SONY
Super HAD CCD™
COLOR



DiD – a Networking Example

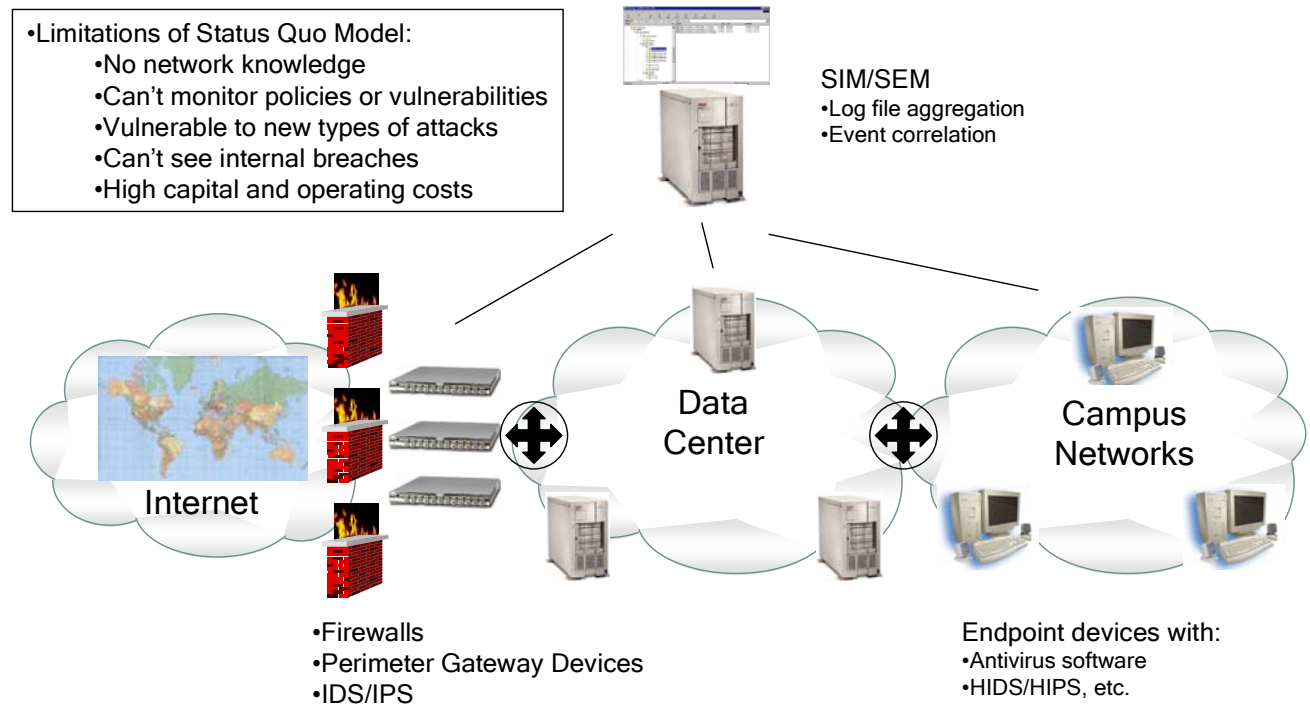
Two years ago, 'best practices'

- Perimeter defenses

- Firewall
- VPN
- IDS

- End node defenses

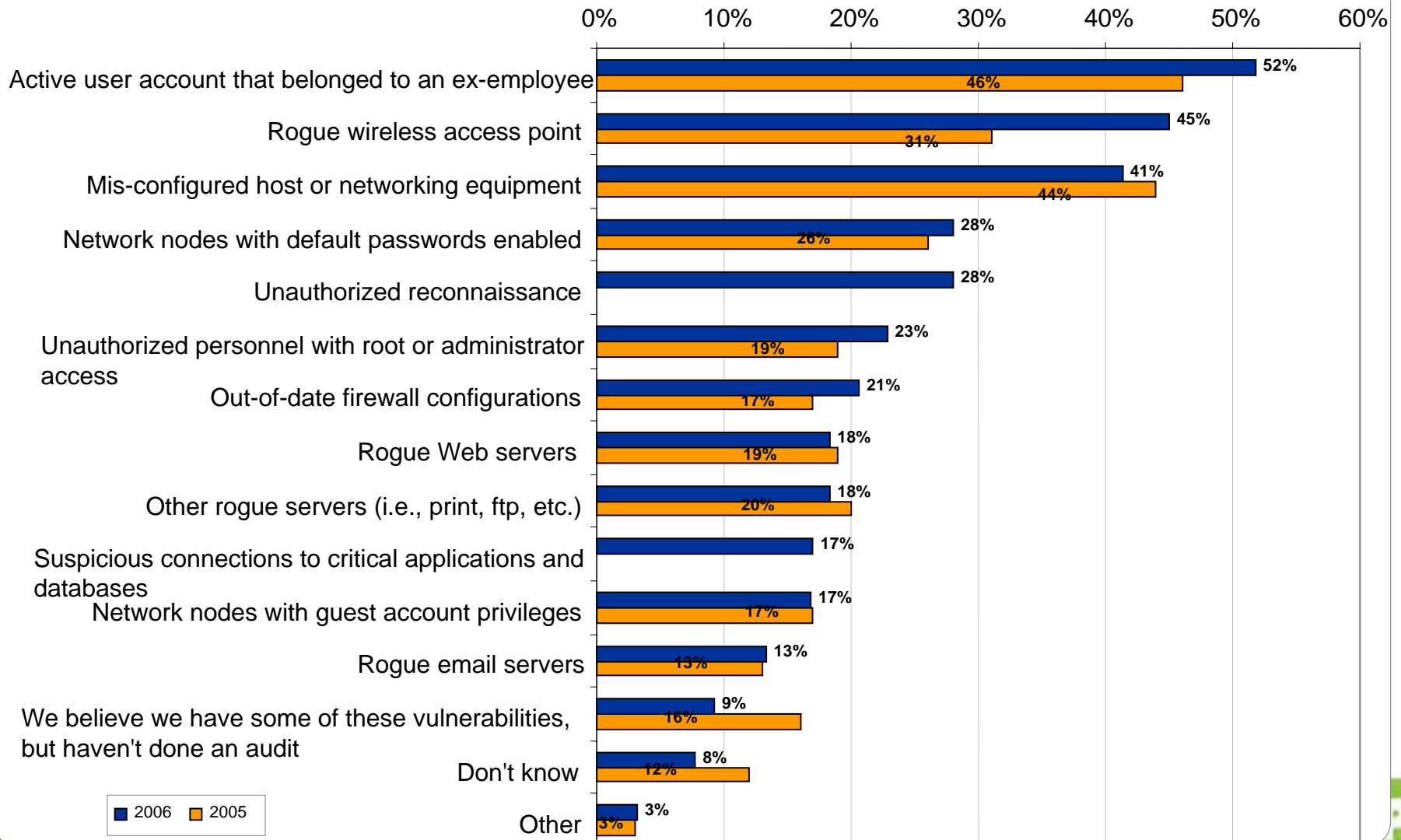
- Anti Virus
- Vulnerability Management
- HIDS



Source: Enterprise Strategy Group

DiD Misses These Scenarios

During the past 12 months, which of the following vulnerabilities did you discover on your network? (Percentage of respondents, N = 218)

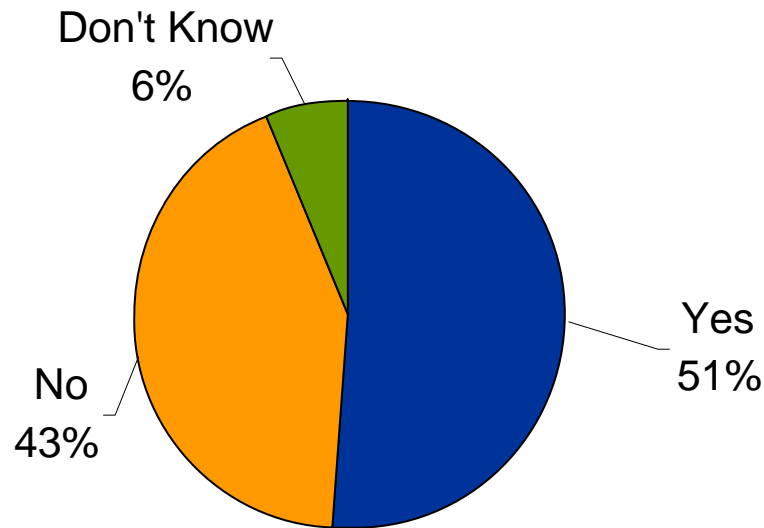


How About Our Recent Attack Vectors?

- **System theft/loss**
 - Fidelity Investments (March)
 - Health Care America (August)
 - Husband and wife I used to work with at VeriSign
 - Veterans Affairs (May)
 - Sovereign Bank (August)
- **BBery proxy** - Discussed at Black Hat this summer
- **Spear Phishing with boutique viruses**
- **Corrupt employees** - Coca-Cola admin tries to sell info to Pepsi-Cola
- **Bad business practices** - Card Systems
- **The average Joe employee** - Leaves his old job for new and copies the entire CRM DB, or CVS repository
- **MS06-040**

Internal Problems Occur

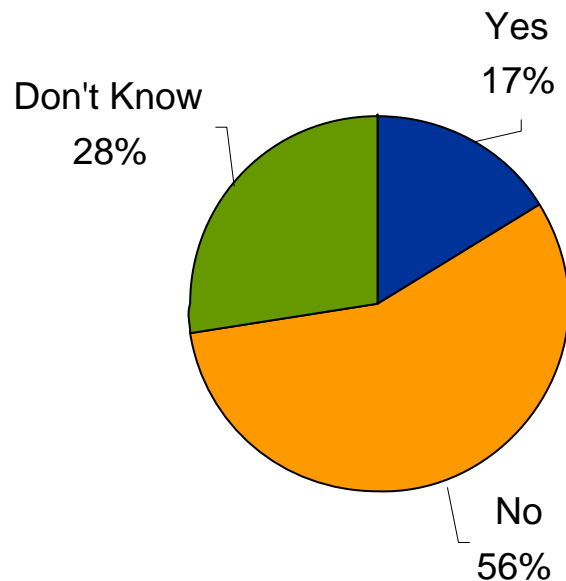
2006: In the past 12 months, has any part of your organization's network been compromised by a worm?



Source: Enterprise Strategy Group 2006 Internal Threat Report

Credentialed Attacks Happen

2006: In the past 12 months, has any part of your organization experienced a targeted attack from an internal source (e.g., employee or credentialed contractor?)



Source: Enterprise Strategy Group 2006 Internal Threat Report

Why Do We Care?

**66% failed to Build and
Maintain a Secure Network**

*Source: VeriSign 2006 paper, "Lessons Learned: Top
Reasons for PCI Audit Failure and How to Avoid Them"*

The Solution

- Return to basics
 - Identify the assets
 - Vulnerability assessment
 - Patch management
 - **Layered defenses**
- Technology is not a panacea
- Work from a real-time view of the network
- Programmatic approaches are the theme
 - A variety of control and detection technologies, diversified approaches

Some Thoughts to Ponder

External Threats ARE Internal Threats

- Hackers go after a single box as a stepping stone into the network
- Once they have this box they are now insider/credentialed users
- From here they typically have easy access to get in further
- Stop the insider and you can stop both the insider and the reach of the outsider

Manage Risk Not Threats

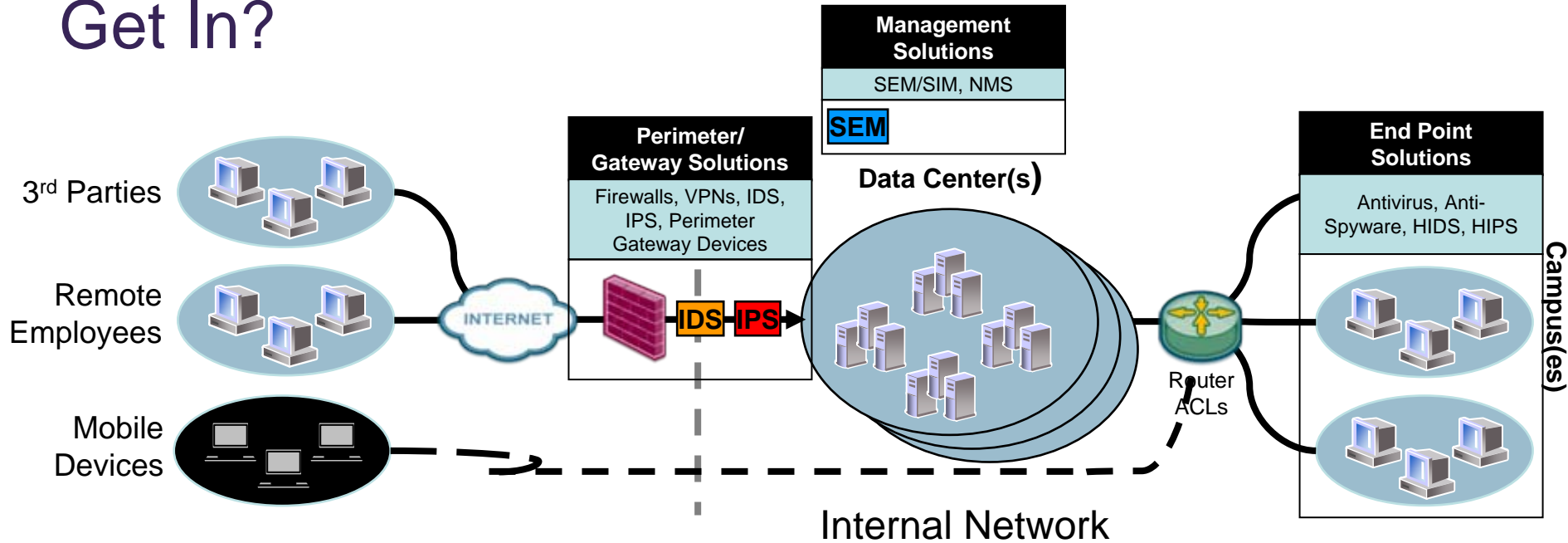
- A *risk* is the possibility that something may happen
- A *threat* is the specific use or attempted use of a risk

- Most technologies are focused on specific threats
- Since it is impossible to know all the possible ways an attack might be tried, *focus on risks rather than threats*
- Focus DiD on network visibility and risk management

How Does Bad Stuff Get In?

Even more attack vectors

How Does Bad Stuff Get In?



- Zero-day attacks / new threats
- Walk-in threats
- Insider breaches
- Misuse of network assets
- Inappropriate access / services

Emerging Technologies

- Network Access Control (NAC) (threat vector)
- Information Leakage Protection (ILP) (risk vector)
- Disk Encryption (threat vector)
- Network Behavior Analysis (NBA) (risk vector)
- Strong authentication (threat vector)

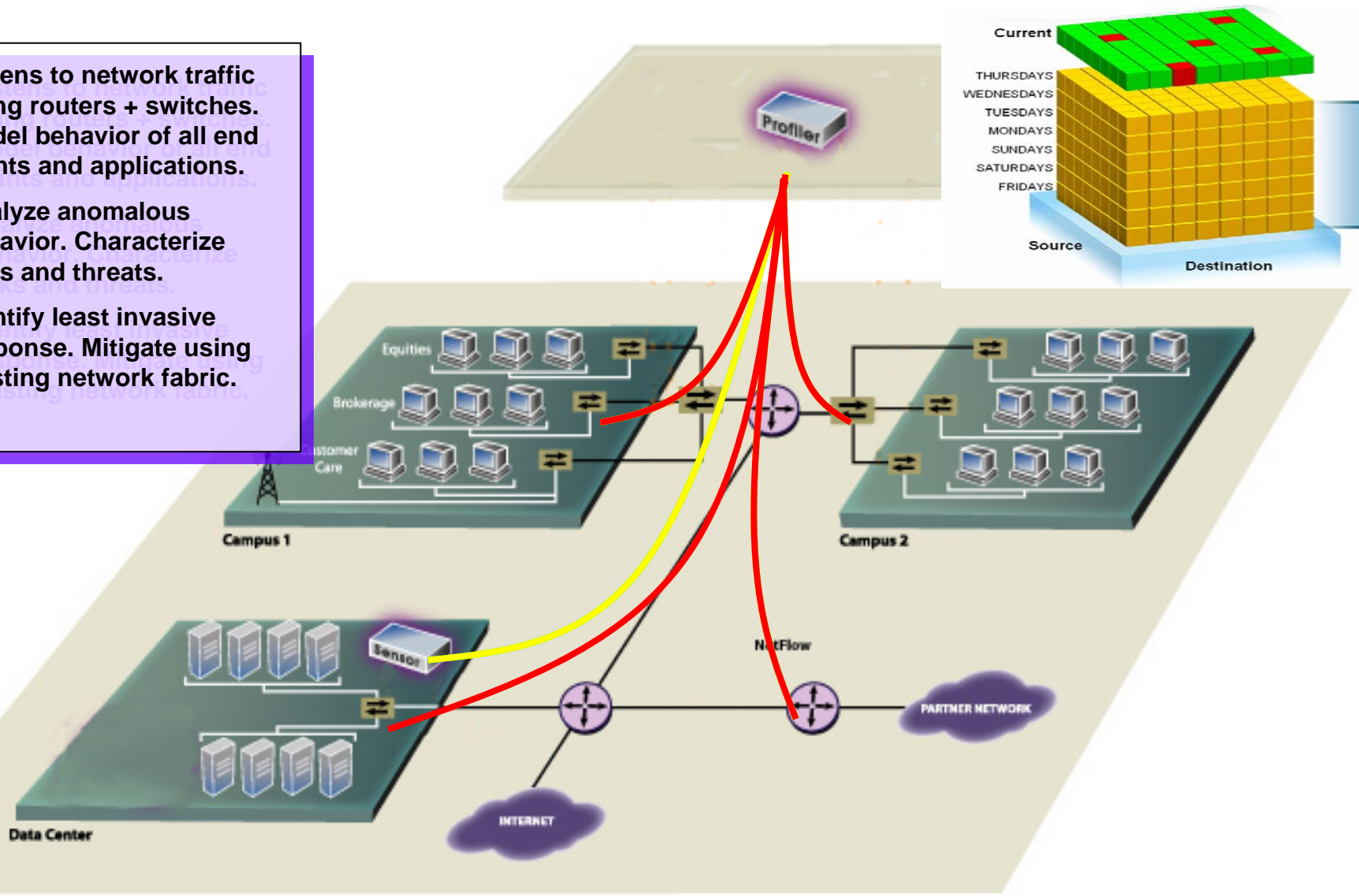
- Lets focus on Risk over Threat protection

What is Network Behavior Analysis (NBA)?

- NBA is a DiD layer between the edge and end node
- Leverages existing router and switch infrastructure for collection and mitigation
- Gain visibility into how systems within the network are used
- Protection from threats the other layers cannot see

How NBA Operates

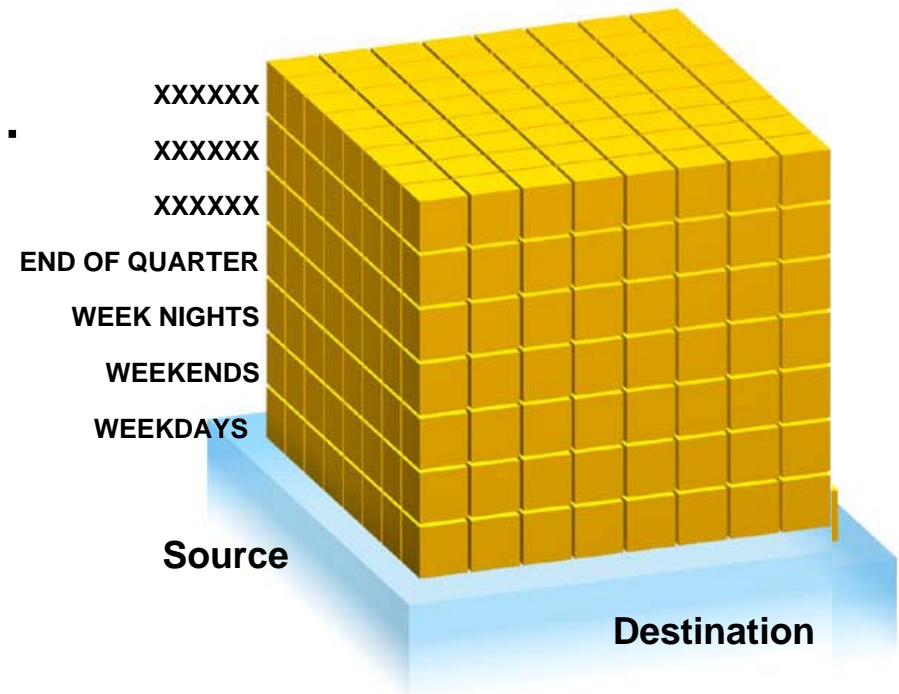
1. Listens to network traffic using routers + switches. Model behavior of all end points and applications.
2. Analyze anomalous behavior. Characterize risks and threats.
3. Identify least invasive response. Mitigate using existing network fabric.



Baselining Network Activity

Build a real-time model of...

- Who talks to whom
- Using what protocols and ports
- Generating how much traffic
- With what frequency
- Who is the client, who is the server
- Which days or time of day



“Use Network Behavior Analysis (NBA) for Better Visibility into Security and Operations Events.”

Title of a Gartner Research Report

Report: G00134030

Published: 9Dec05

What People are Saying About NBA

- “Network Behavior Analysis systems are the new foundation of Defense-in-Depth architectures”
Enterprise Strategy Group, November 2005
- “By year-end 2007, 25% percent of large enterprises will employ NBA as part of their network security strategy”
Gartner Research, December 2005
- “Today’s complete layered security solution should include IDS, IPS, NBA & endpoint security to ensure security posture pre and post network authorization and authentication”
Yankee Group, December 2005

Keys to Remember

- Security is a marathon
- Security is everyone's responsibility
- Defense is the stronger form of waging war

- A successful security initiative will deliver value across the entire IT organization
 - Because end users only care that it works

Value Across the IT Organization

Network Security	Network Operations
<ul style="list-style-type: none">• Detect and mitigate worms, internal threats + unauthorized reconnaissance• Identify unauthorized services• Identify mis-configurations• Identify misuse of services	<ul style="list-style-type: none">• Troubleshoot network slowdowns• Identify the impact of a policy change• Enable rapid response in a crisis• Detect and mitigate operational threats
Network Engineering	Audit + Compliance
<ul style="list-style-type: none">• Server consolidation• Network segmentation• Disaster recovery• Services inventory & usage	<ul style="list-style-type: none">• Assess regulatory readiness• Identify and respond to incidents• Enforce defined controls over critical assets

Internal Security

Insider Breach



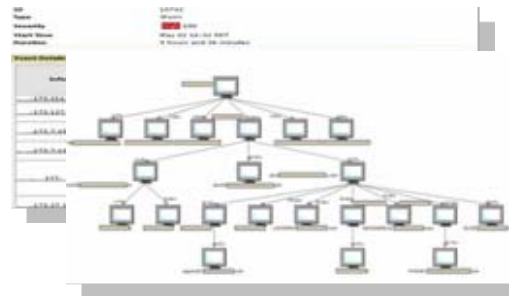
Worm Outbreak



Mitigation Impact



Metric	Effect on Severity
The attacker has not previously accessed the victim.	+20
The average host in custom group <u>Contractors</u> connects to 0.00% of hosts in <u>Contract-CEs</u> .	+20
There were 2 TCP connections in one time period.	+5
At least one port was not well known.	0
1 new ports were used.	+10
There were 0.02 connections per second and 88 bytes per connection.	0
The victim normally receives 0 connections per second.	0
The attacker normally makes 0.00 connections per second.	0
The attacker has been up for 1,107,480 seconds.	0
The victim has been up for 1,107,480 seconds.	0
The attacker has not subsequently made a connection to an outside host.	0



Proposed Actions	Methods	Port	Affected hosts
Host #	<input type="checkbox"/> Router	<input type="checkbox"/> Switch	
2.2.3.4	<input type="checkbox"/> s+ 7200-1	<input type="checkbox"/> t: 10	2/7 ↓
Desktop	<input type="checkbox"/> s+ 7200-1	<input type="checkbox"/> t: 10	2/1 ↓
2.2.3.2	<input type="checkbox"/> s+ 7200-1	<input type="checkbox"/> t: 10	2/5 ↓
Desktop	<input type="checkbox"/> s+ 7200-2	<input type="checkbox"/> t: 15	3/7 ↓
2.2.3.3			
Desktop			

Comm. Recalculate

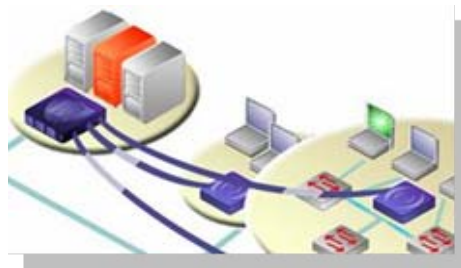
NBA delivers value here

Compliance

Developers in Production Environment



Unsecured Services used on PCI Servers



Archive of Historical Activity & Connections



Event Detail Report

Event Summary

ID: 15179
 Type: Rule Based Event
 Severity: CRITICAL
 Start time: Feb 09 00:00:00
 Duration: 6 hour and 7 minute
 Vulnerability scan: No scan

Event Details

Reason: PCI violation
 Description: Non-PCI client access a PCI system.
 Rule Summary:
 Rule is a UserMonitor rule. It looks at traffic to Rgn between clients and servers.
 Total aggregate traffic between clients and servers: 50,279 Kbp (2063.328)

Alerts

Alert	Group
15179, 15179	DefaultAlert

Services

Alert	Group
15179, 15179, 15179	DefaultAlert

As shown by rules on this event

Source: Add a rule to suppress this alert for a specified period of time.
 Action: Use the 'Threshold' feature to change settings such that similar behavior could not generate an alert.

Traffic Report

Historical traffic between Applications_Servers group and any host using t
 No entries found.

Summary of traffic by Critical Server Groups groups

Group	Avg Bits ↓	(%)	Avg
No entries found.			

* Traffic volumes are reported for each group. For a connection between i
 traffic to Group B is also Group B's incoming traffic from Group A. Because
 connection, column totals are twice the actual network traffic.

Flow summary of Historical traffic between Applications_Servers grou

Start	End	Protocol	Client	Client MAC	Client Switch	Server	Server
No entries found.							

History of Historical traffic between 172.31.5.35 and any host (Showing 100 of 1241)

Start	End	Protocol	Client	Client MAC	Client Switch	Server	Server MAC	Server Switch	Bytes Request	Packets Request	Flags	Bytes Response	Packets Response
16 Feb 08 00:10:31	16 Feb 08 00:10:31	Tcp	172.31.5.35	0874	MS	172.31.5.116	449	MS	6,503	45	SRQ	4,432	41
19 Feb 08 00:21:37	19 Feb 08 00:21:37	Tcp	172.31.5.35	4922	MS	172.31.5.123	1395	MS	450,430	1,003	PSHA	98,276	432
17 Feb 08 00:11:04	17 Feb 08 00:11:04	Tcp	172.31.5.35	4955	MS	172.31.5.123	1395	MS	40	1	SRQ	31	2,848
10 Feb 08 00:00:12	10 Feb 08 00:00:12	Tcp	172.31.5.35	4977	MS	172.31.5.123	1395	MS	1,952	13	PSHA	3,669	14
13 Feb 08 00:00:13	13 Feb 08 00:00:13	Tcp	172.31.5.35	4579	MS	172.31.5.123	1395	MS	1,432	25	PSHA	28,104	35
13 Feb 08 00:00:13	13 Feb 08 00:00:13	Tcp	172.31.5.35	4579	MS	172.31.5.123	1395	MS	1,638	8	PSHA	779	8
13 Feb 08 00:00:13	13 Feb 08 00:00:13	Tcp	172.31.5.35	4561	MS	172.31.5.123	1395	MS	569	7	PSHA	584	7
13 Feb 08 00:00:13	13 Feb 08 00:00:13	Tcp	172.31.5.35	4562	MS	172.31.5.123	1395	MS	564	7	PSHA	584	7
13 Feb 08 00:00:13	13 Feb 08 00:00:13	Tcp	172.31.5.35	4564	MS	172.31.5.123	1395	MS	596	7	PSHA	584	7
13 Feb 08 00:00:13	13 Feb 08 00:00:13	Tcp	172.31.5.35	4565	MS	172.31.5.123	1395	MS	592	7	PSHA	584	7
13 Feb 08 00:00:13	13 Feb 08 00:00:13	Tcp	172.31.5.35	4569	MS	172.31.5.123	1395	MS	555	6	PSHA	584	7
13 Feb 08 00:00:13	13 Feb 08 00:00:13	Tcp	172.31.5.35	4590	MS	172.31.5.123	1395	MS	555	7	PSHA	584	7
13 Feb 08 00:00:14	13 Feb 08 00:00:14	Tcp	172.31.5.35	4580	MS	172.31.5.123	1395	MS	570	7	PSHA	626	8
13 Feb 08 00:00:14	13 Feb 08 00:00:14	Tcp	172.31.5.35	4583	MS	172.31.5.123	1395	MS	1,592	10	PSHA	4,424	12
13 Feb 08 00:00:14	13 Feb 08 00:00:14	Tcp	172.31.5.35	4588	MS	172.31.5.123	1395	MS	1,051	15	PSHA	2,292	11
14 Feb 08 00:00:14	14 Feb 08 00:00:14	Tcp	172.31.5.35	4591	MS	172.31.5.123	1395	MS	595	7	PSHA	584	7
14 Feb 08 00:00:14	14 Feb 08 00:00:14	Tcp	172.31.5.35	4592	MS	172.31.5.123	1395	MS	559	7	PSHA	584	7
14 Feb 08 00:00:14	14 Feb 08 00:00:14	Tcp	172.31.5.35	4593	MS	172.31.5.123	1395	MS	559	7	PSHA	584	7
14 Feb 08 00:00:14	14 Feb 08 00:00:14	Tcp	172.31.5.35	4594	MS	172.31.5.123	1395	MS	570	7	PSHA	585	7
17 Feb 08 00:00:19	17 Feb 08 00:00:19	Tcp	172.31.5.35	4595	MS	172.31.5.123	1395	MS	1,176	12	PSHA	3,434	12

NBA delivers value here

Application Availability

M&A Activity



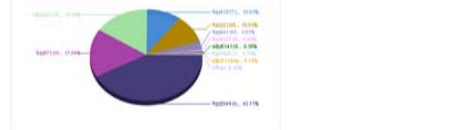
Profile & Fingerprint New Applications



Monitor Application Profiles



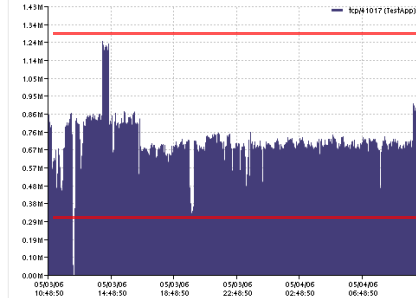
Traffic Report
Historical traffic between Applications_Servers group and any host from May 03 2006 10:22:49 PM to May 03 2006 10:22:49 PM



Service	Req.Bits/s	(%)	Res.Bits/s	(%)	Req.Connections	(%)
tcp/41017	1,147,519/s	(47%)	468/s	(4%)	0	(0%)
tcp/8080	1,115,999,717	(17%)	156/s	(14%)	0	(0%)
udp/53	1,179,193,717	(18%)	98/s	(9%)	0	(0%)
tcp/8080	792,610,019	(10%)	112/s	(10%)	0	(0%)
tcp/443	79,973,019	(10%)	136/s	(12%)	0	(0%)
tcp/443	299,052,019	(4%)	42/s	(4%)	0	(0%)
tcp/8080	46,452,019	(0.44%)	70/s	(0%)	1/0	(0%)
tcp/443	24,929,019	(0.34%)	5/s	(0.40%)	0	(0%)
tcp/8080	14,470,019	(0.19%)	2/s	(0.19%)	0	(0%)
tcp/8080	14,040,019	(0.19%)	11/s	(0.19%)	0	(0%)
tcp/443	13,940,019	(0.19%)	23/s	(2%)	0	(0%)
tcp/8080	9,304,019	(0.12%)	54/s	(0.50%)	0	(0%)
tcp/8080	1,307,019	(0.01%)	8/s	(0.01%)	1/0	(0%)
tcp/80	1,300,019	(0.01%)	13/s	(0.01%)	0	(0%)
tcp/8080	840,019	(0.01%)	56/s	(0.01%)	0	(0%)

Traffic Report

Historical traffic between Test_Servers group and any host using TCP/41017 from May 03 2006 10:22:49 PM to May 03 2006 10:22:49 PM



Rule Based Event

Identification

Name: New App unavail
Description: Application unavailable
Type: Check / Server

Schedule

Start to run rule: Any Week Mon Tue Wed Thu Fri Sat Sun
Start time: 00:00:00
End time: 24:00:00

Client Host

Host Selection: Any Watch List Outside List
Host Statistics: Track In Aggregate

Server Host

Host Selection: Any Watch List Outside List
Host Statistics: Track In Aggregate

Service

Service Selection: Any Watch List Outside List
Service: tcp/41017

Threshold

Level: Lower Limit
Threshold: 00:00:00
Duration: 00 Hours 01 Minutes
Severity: High
Notification: Low: Default, Medium: Default, High: Default

NBA delivers value here

So NBA is the Answer?

- Sorry, there are no silver bullets.
 - DiD is about layers, and NBA adds an internal layer

NBA

- ▶ **Visibility**: into how the network is being used
- ▶ **Protection**: from worms and insider breaches
- ▶ **Compliance**: through audit & enforcement of internal controls

Emerging Problems

- Tight budgets
- Network and security convergence
- Telecom/VoIP
- IP enabled facilities
- Compliance
- Wireless/mobile devices
- Lack of skilled help

Recent High Stress Scenarios

- Rogue contractor stealing data
- Developers accessing production systems
- Day Zero worm detection
 - Who was patient zero?
- Worm mitigation efforts disabling VoIP call center
- An employee sets up their own Web server which, un-patched and stealthed
- Telnet being used to connect to PCI servers
- Auditor requests proof that no unauthorized connections were made to key servers
- Help desk is swamped with complaints that the network is slow or critical applications are unavailable
- An acquisition must be integrated without network documentation or willing assistance
- A new service to be rolled out – without any visibility into how it will affect the network

Summary

- DiD must address edge & end node, as well as internal/credentialed user threats
- Increased spend on legacy technologies has not helped
- Approximately 50% of your threats and 85% of your \$ lost come from credentialed threats
- NBA solutions are a viable element in DiD strategies
- Understanding your network will not only improve security, but deliver value across IT



Additional information
available at:
www.mazunetworks.com

Q&A

How can you implement NBA
into an existing network that is
likely compromised already?

How does this apply in the face of growing application encryption?

How else might one get visibility into the network?

Why not deploy more firewalls and IDS into the core of the network?