

Mazu Networks

Eliminating the tradeoff between security and accessibility

Presentation to ACSAC

December, 2003



MazuTM
NETWORKS

Profile | Plan | Protect

Afsana Akhter
Director, Solutions
Engineering

Josh Wolfe
Director, Federal Sales

Mazu Networks

Who are we? Behavioral security solutions that profile, plan and protect enterprise and government networks.

Established in 2000. HQ in Cambridge, MA. Offices in New York, Washington DC, San Francisco and London.

What makes us unique? Real-time traffic profiling technology based on MIT research (21 patents pending) . First to provide detailed real-time insight into enterprise-wide network behavior

Our Value: Eliminate the tradeoff between security and accessibility – enabling organizations to broaden access to critical applications with less risk and fewer resources.

Mazu's Solutions

Enforcer Perimeter-based security appliance.

Protects against traffic-based attacks by profiling traffic flowing through the network and providing highly accurate detection and precise filtering of attack traffic.

Profiler Platform to secure critical applications + processes

Provides real-time profile of how network assets and services being used, and leverages this insight for detection, response + recovery and hardening access.

Case Study: Wider Access to Critical Apps + Data

Client: Fortune 50 Financial Services Company

2 Offshore Contractor

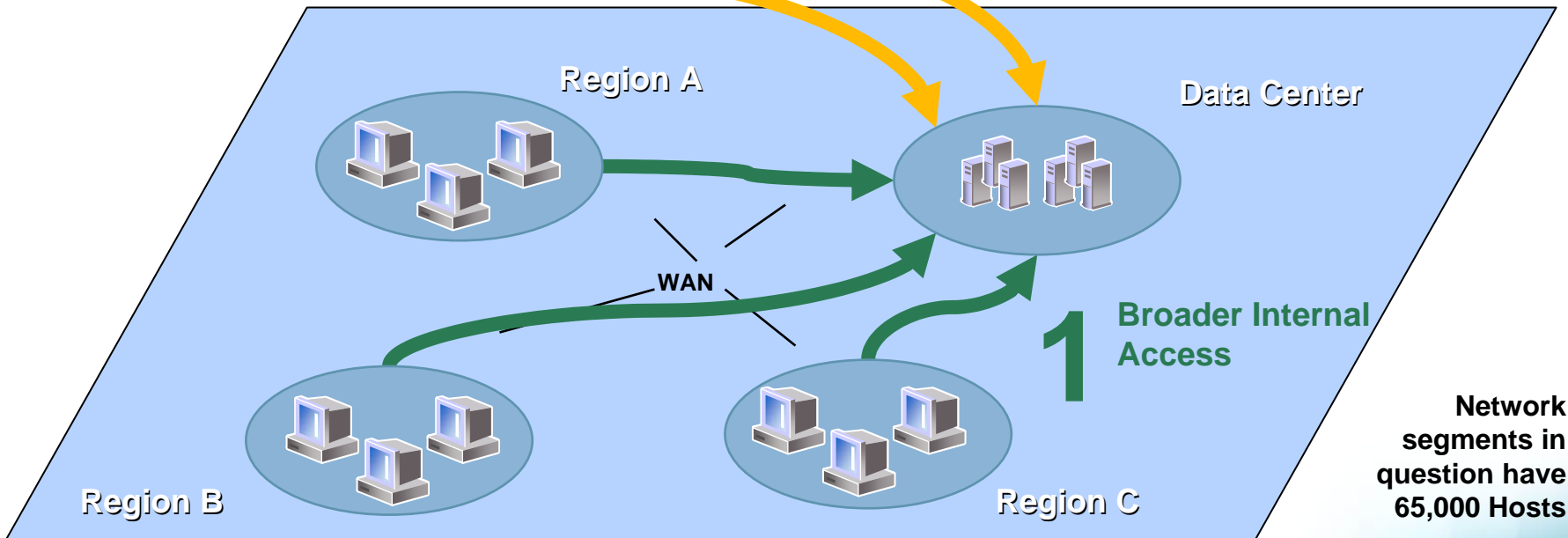
3 Remote Users

Providing Access is straightforward – securing introduces new risks + costs

- Large # of Credentialed Users
- Remote + 3rd Party Users
- Mobile + Wireless Devices

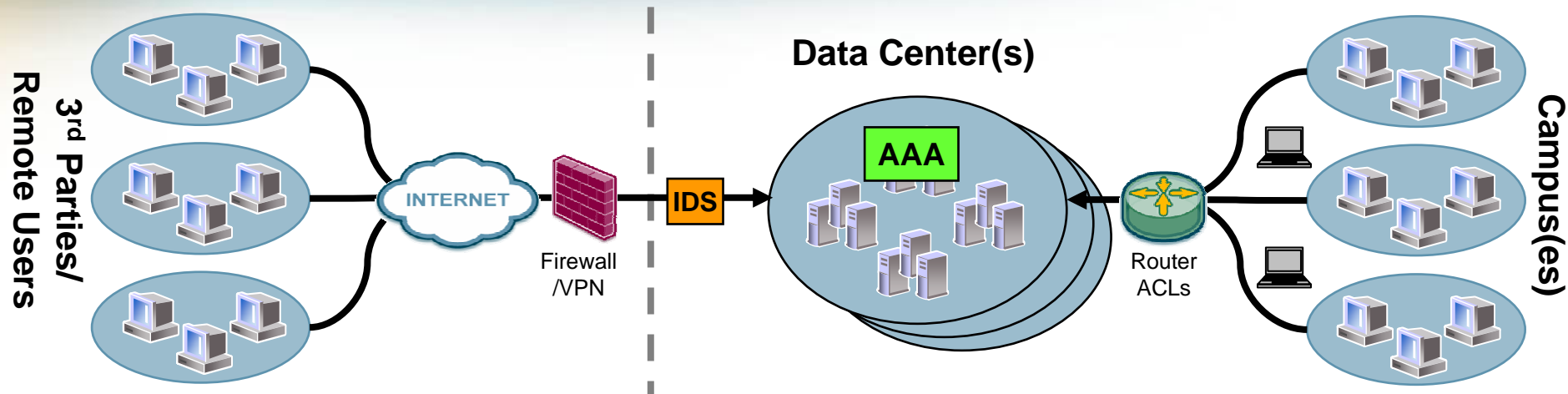
External Hosts and Applications

Internal Hosts and Applications



Network segments in question have 65,000 Hosts

Wider Access = New Risk + Work



Increasing...

- # of credentialed users
- # of remote + 3rd party users
- # of applications + services
- # of mobile devices

Perimeter Vs Core

- Successful techniques at perimeter prove less so inside the network
- Different set of risks
- Different set of work

New Risks + New Workload

Risks

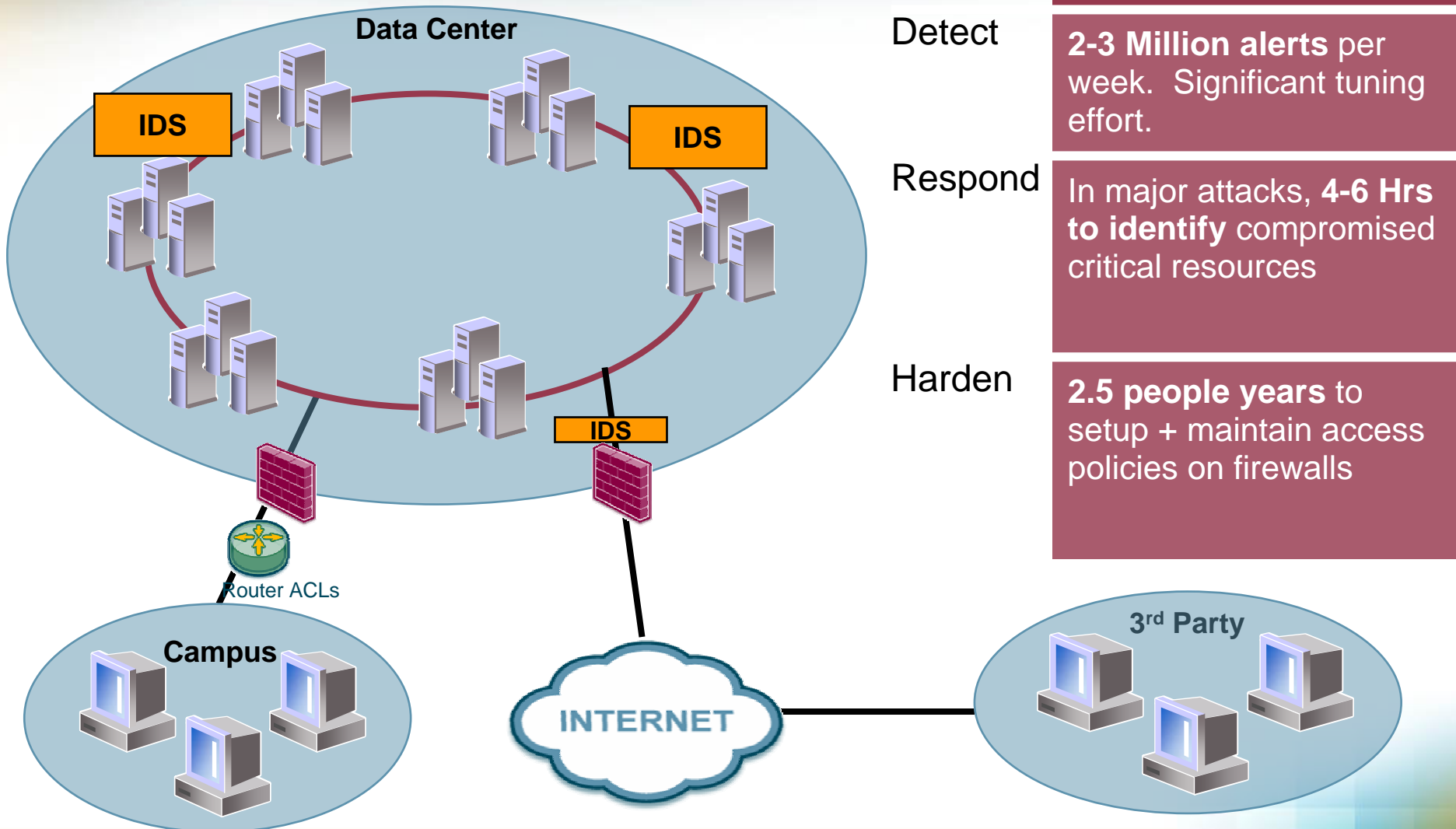
1. Detecting 0-day attacks, trojans + attacks entering via credentialed hosts
2. Response + Recovery to large scale attacks such as worms, DDoS, etc.
3. Monitoring acceptable usage policy, unauthorized access + stealthy scans

+

Workload

1. Quantity of false positives + duplicate alarms
2. Lack of actionable info to respond + recover
3. Complexity of maintaining tight access policy on firewalls + routers

Case Study: The Initial Solution



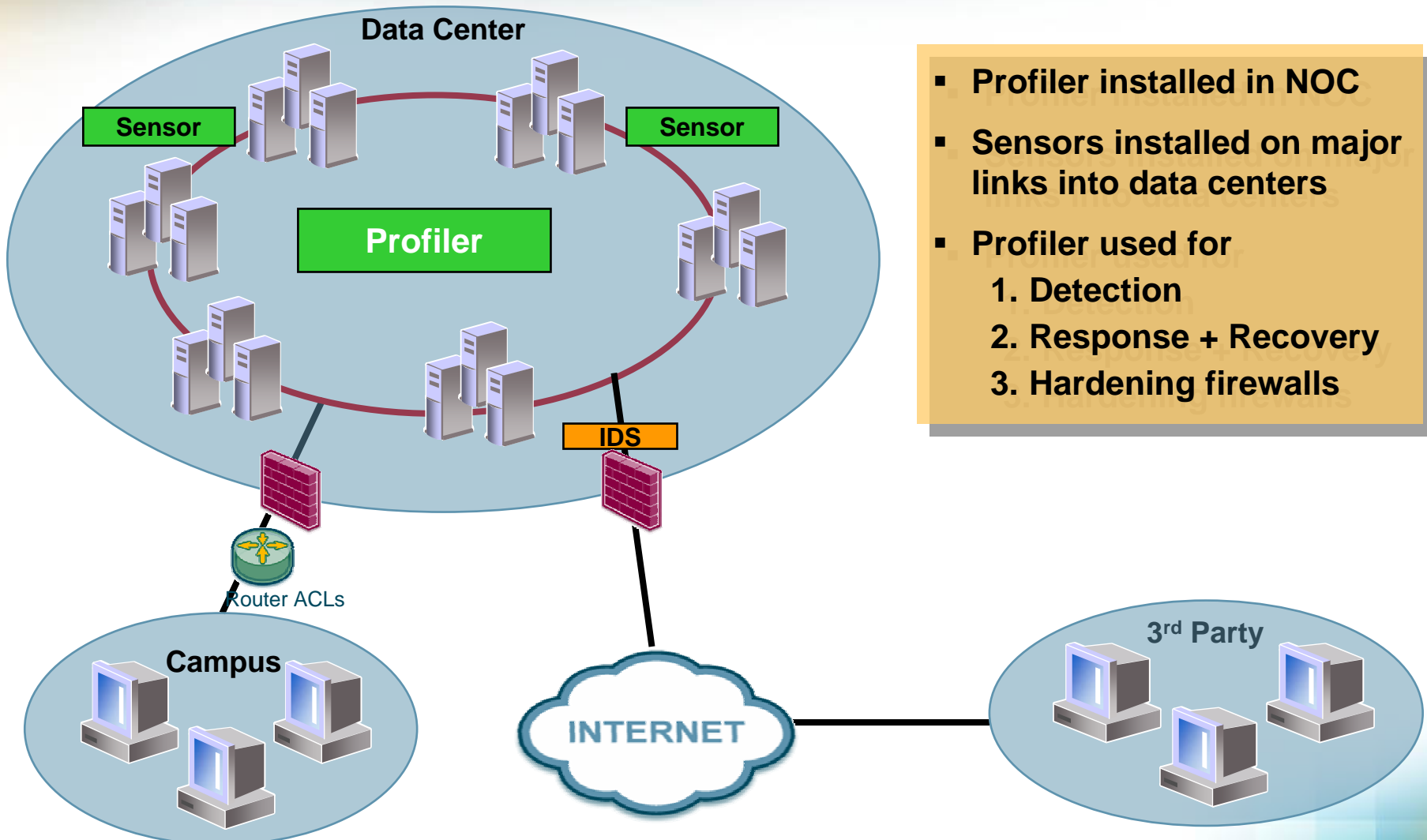
Before

Detect
2-3 Million alerts per week. Significant tuning effort.

Respond
In major attacks, 4-6 Hrs to identify compromised critical resources

Harden
2.5 people years to setup + maintain access policies on firewalls

Case Study: The Profiler Solution

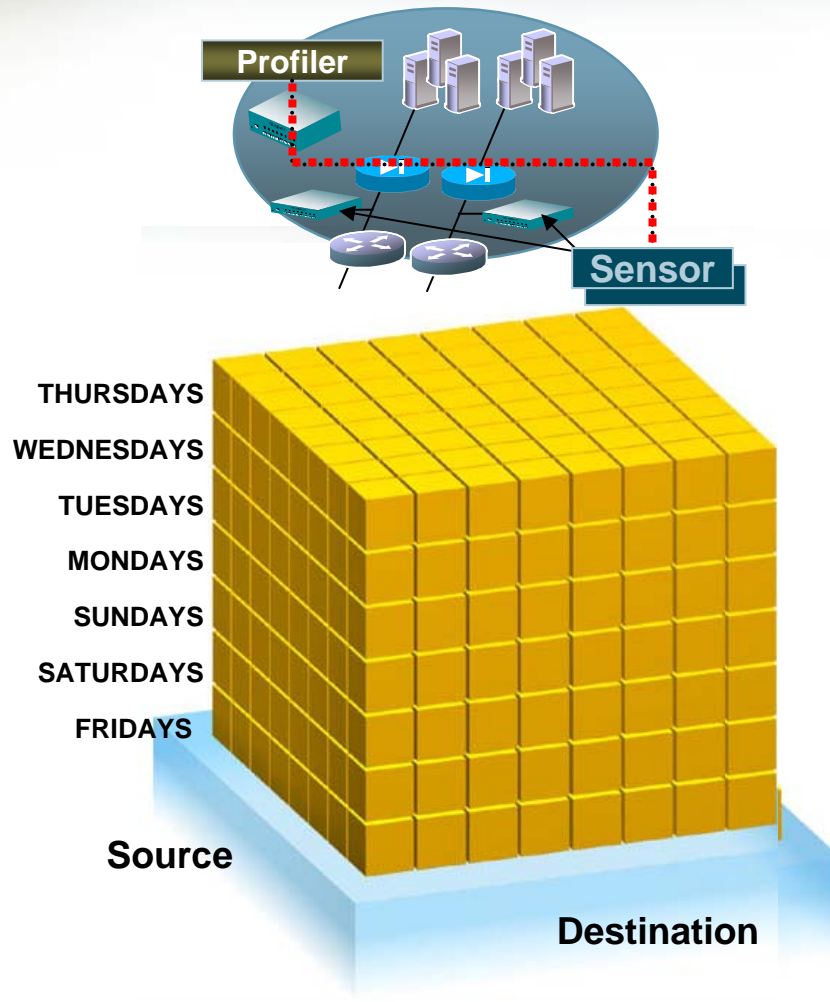


Case Study: Results

	Before	After
Detect	2-3 Million alerts per week.	2-3 Hundred alerts / week → 99% Reduction
Respond	In major attacks 4-6 Hrs to identify compromised critical resources	2-3 minutes to identify + prioritize compromised and their dependants → 99% Reduction
Harden	2.5 people years to setup + maintain access policies on firewalls	0.3 people years → 88% Reduction

MCube: Core Profiler Technology

Baseline | Group | Maintain



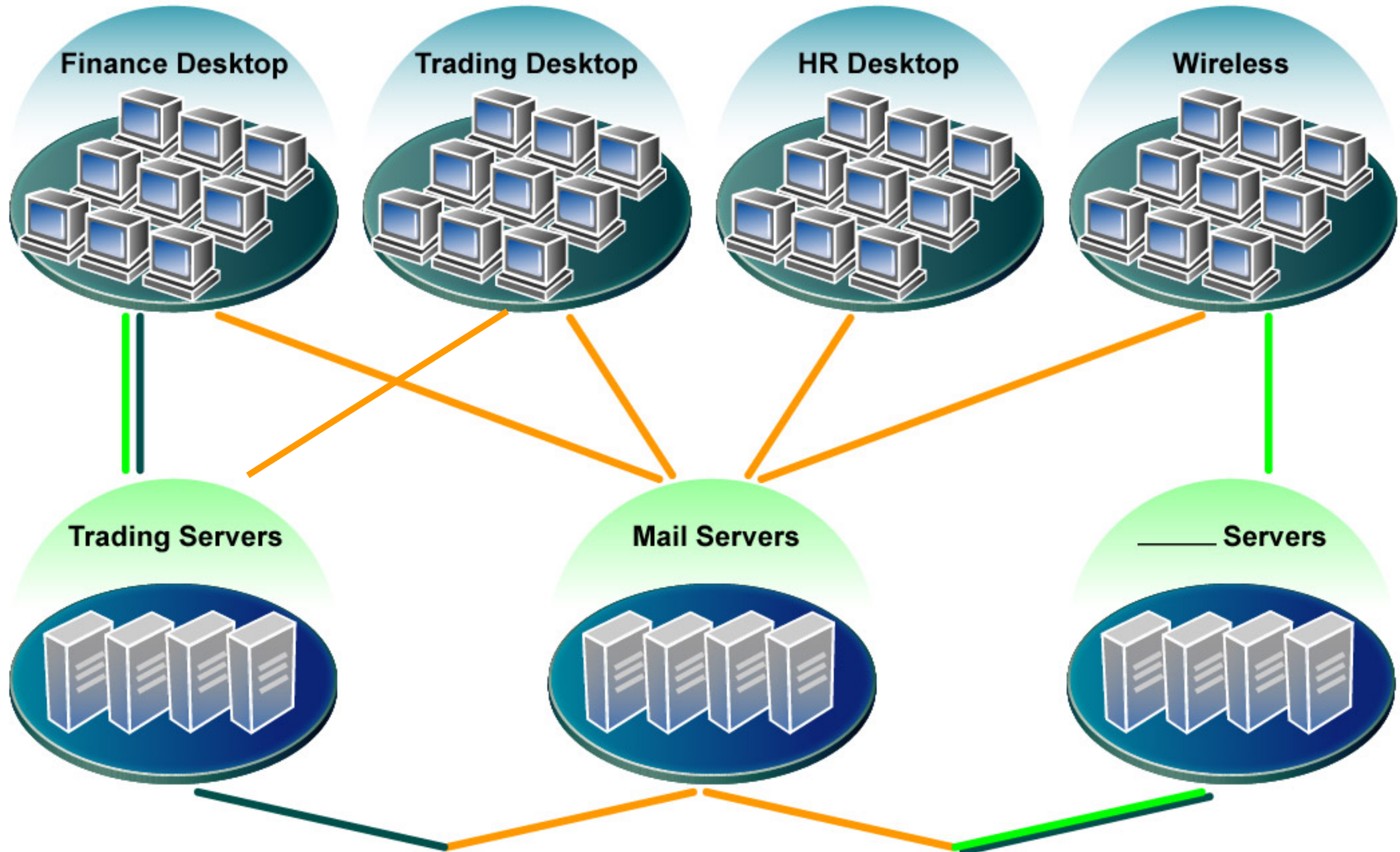
Building a real-time model of...

- *Who talks to whom*
- *Using what protocols*
- *Over which ports*
- *Which days or time of day*
- *Consuming what services*
- *Generating how much traffic*
- *With what frequency*
- *Who is a “consumer” of this asset or service*

Real-time Insight Understand How Your Network is Used

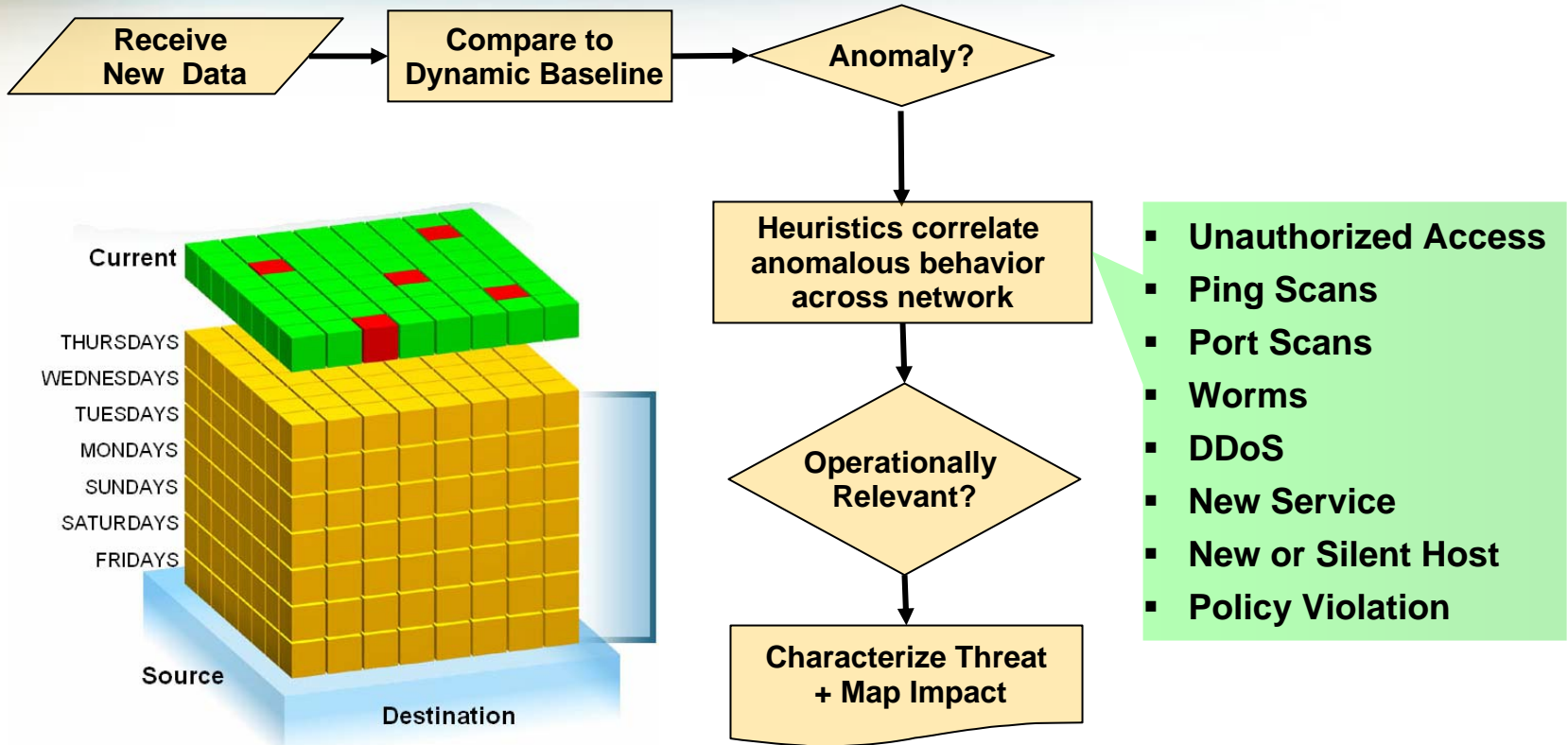


Baseline | Group | Maintain



Highly Accurate Attack Detection

Detect | Respond | Harden



Identifying events based on observing and analyzing changes in how the network is being used yields highly relevant alarms

Critical Solution Attributes

Risks	1	Visibility	Monitor + understand how critical network assets are being utilized.
	2	Detection	<ol style="list-style-type: none"> 1. Zero-day attacks, trojans + threats from credentialed hosts 2. Worms, unauthorized access, DDoS, scans 3. Violations of acceptable usage policy
Resources	3	Workload	<ol style="list-style-type: none"> 1. Reduce false positives + duplicate alarms 2. Actionable info to respond and recover from attacks 3. Automate definition access policy on firewalls and routers
	4	Integration	Integrate with legacy systems and processes including NMS, DHCP server, Asset Management System, Radius Server
Scale	5	Scalability	Handle relevant # of hosts inside and outside the enterprise (profile, model, visualize). Control cost + effort to roll out.

Summary

1. The Mazu Profiler reduces the risk and workload associated with securing broader access to critical applications in enterprise and government networks
2. Profiler addresses detection, response + recovery, and hardening access policy on firewalls + routers
3. Profiler's unique value comes from MCube technology that provides detailed real-time insight into how networks are actually used – and enables greater accuracy, efficiency + scalability.

Mazu Networks

Eliminating the tradeoff between security and accessibility

Presentation to ACSAC

December, 2003



MazuTM
NETWORKS

Profile | Plan | Protect

Afsana Akhter
Director, Solutions
Engineering

Josh Wolfe
Director, Federal Sales