Consolidation

UTM / NAC and the Need for Greater Visibility

kurtis minder
and
steven ocepek

questions@kurtisminder.com

Introduction

Kurtis E. Minder, Technical Sales Professional

Companies:

Roles:

- Security Design Engineer
- Systems Engineer
- Sales Engineer
- Salesperson
- Business Development
- Global Account Manager

Actual work:

- Installation / Configuration
- Design
- Support
- Product development / POC
- Audit
- Penetration testing
- Sales / BD

CISSP Certification

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security CISSP
- Security Architecture and Design
- Telecommunications and Network Security

The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.

Agenda

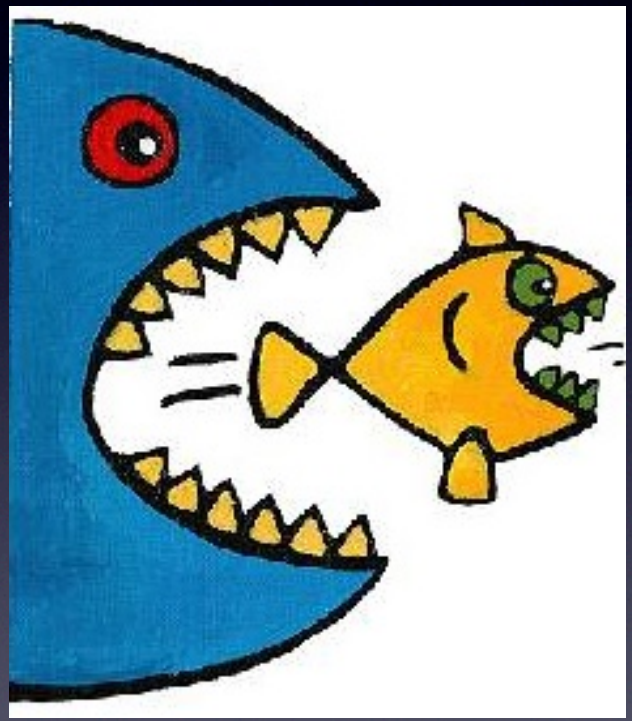
- Introductions
- 3 Letter Acronyms and a Cloud (review)
- History of Security Device Management
- The SIM / SEIM / SEAM

3 Letter Acronyms and a Cloud

(Non-Comprehensive InfoSec Industry Update)

What is going on?

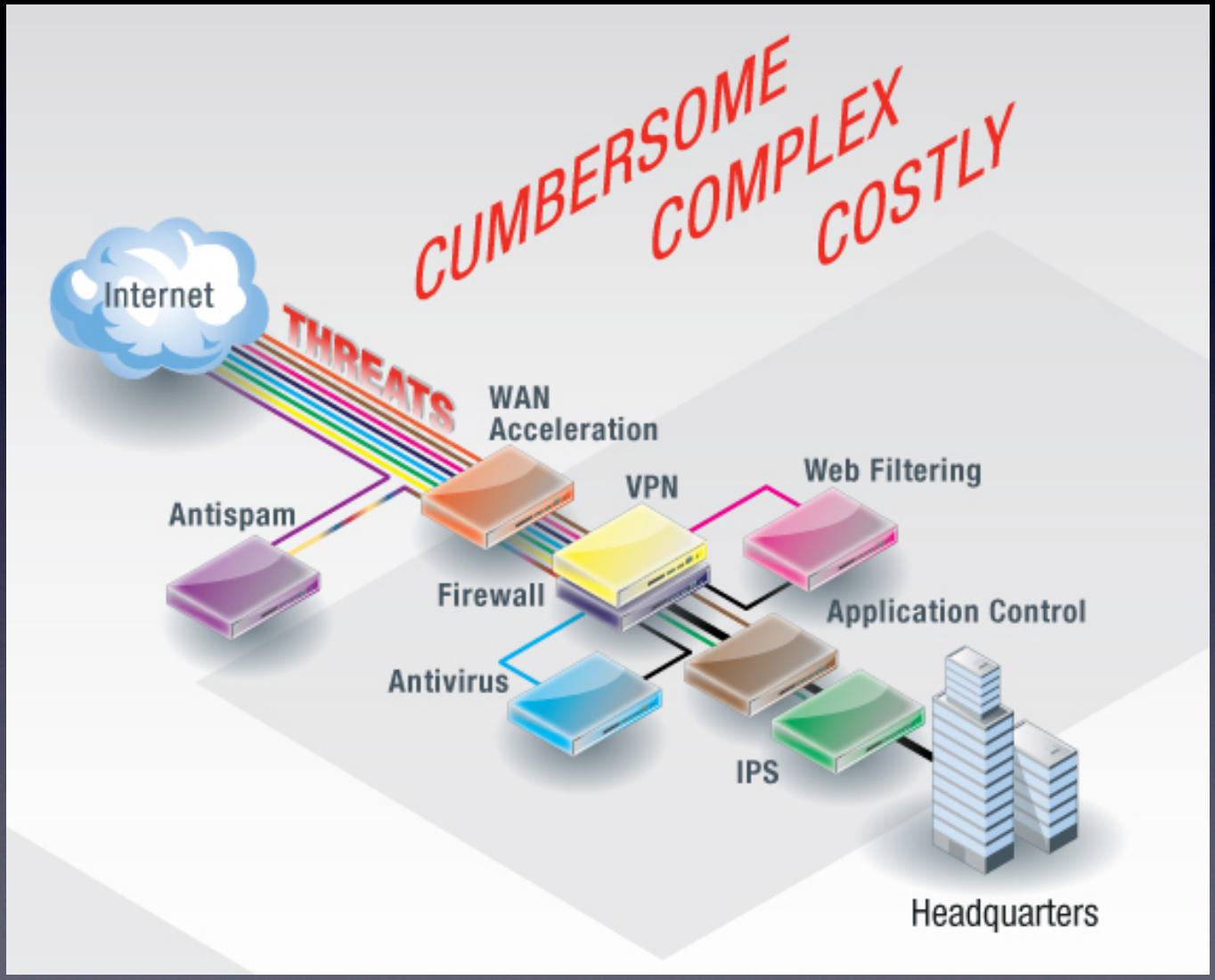
- Vendor consolidation
- Move toward single platform solutions
- NAC, What happened?
- Managed services approach catching on in enterprise
- Cloud cloud cloud cloud



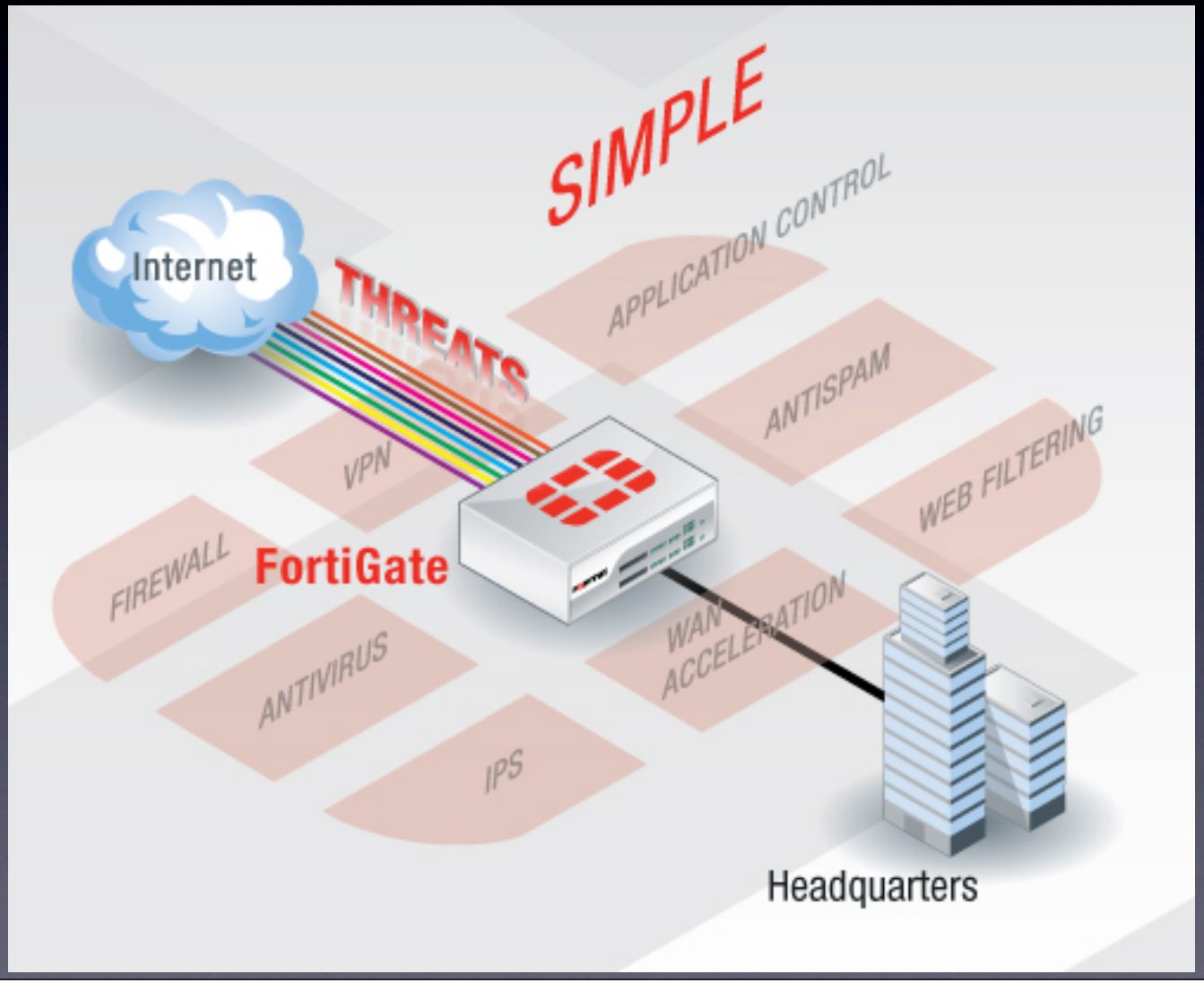
U T M

- Unified Threat Management Goes Bigtime
  - Fortinet Maintains the Lead
  - Cisco and Juniper Follow
- Why UTM?
  - Consolidated Approach
  - Economic Benefits
  - Architectural Benefits
  - Security Benefits (Best of breed not best after all?) <-- Not Rhetorical

The Perimeter

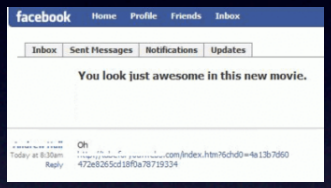


The Consolidated Perimeter



Integrated Security in Action

Problem:



"Innocent" Video Link:
Redirects to malicious Website

"Out of date" Flash player error:
"Download" malware file

Error message:
"Drops" copy of itself on system and attempts to propagate

Solution:

Integrated Web Filtering
Blocks access to malicious Website

Network Antivirus
Blocks download of virus

Intrusion Protection
Blocks the spread of the worm

N A C

- Why Network Access Control
  - Business Needs (Started with SSL VPN, no?)
  - Security Needs
  - Compliance Needs - PCI?
- What Happened, Man?
  - Is NAC Dead?
  - Where is it going? (Unicorn)

Special note to JJ and Shimmy, thanks.
http://www.securityuncorked.com - http://www.stillsecureafterallthoseyears.com

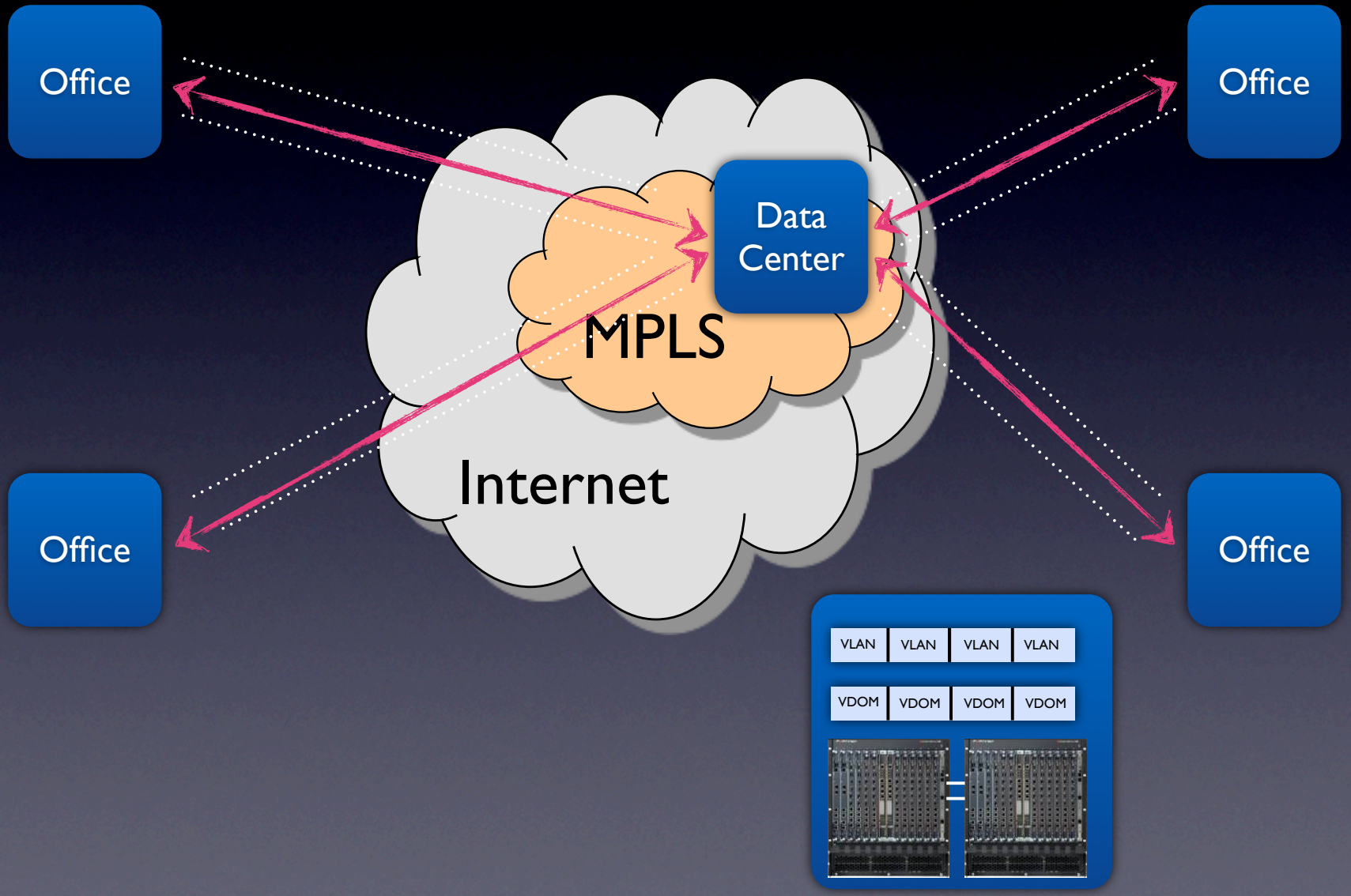
M S S

- Managed Security Services, Why?
  - Operational Benefits
  - Capital Expenditure Benefits
  - “Pure play” vs. Bundles Services
  - Cloud vs. CPE

Cloud

- Cloud Security, what does that mean?
  - "Clean Pipe"
  - Shared Services Model
  - Integrating with the carrier backbone (MPLS)
- Cloud Computing
  - SAAS, IAAS, PAAS need Security!
  - How to provision? Is it VM? Is it appliance?

Cloud Security Example



The Visibility Problem

The Problem

NAC Data

Intrusion Prevention Event Data

Too Much Data

NetFlow Data

System Event Data

Anti-Virus Data

Web Content Filter User Data

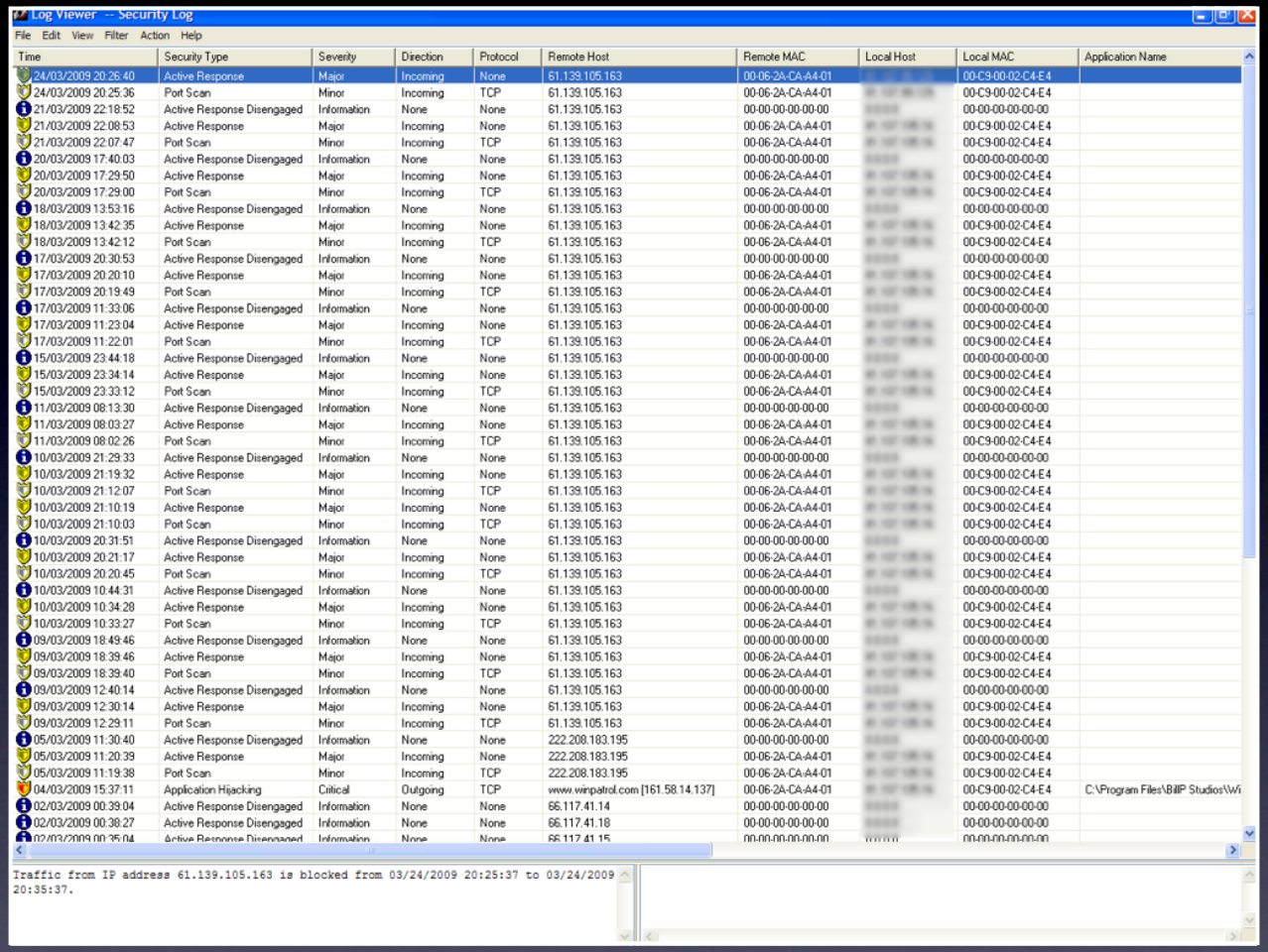
Firewall Event Data

VPN User Data

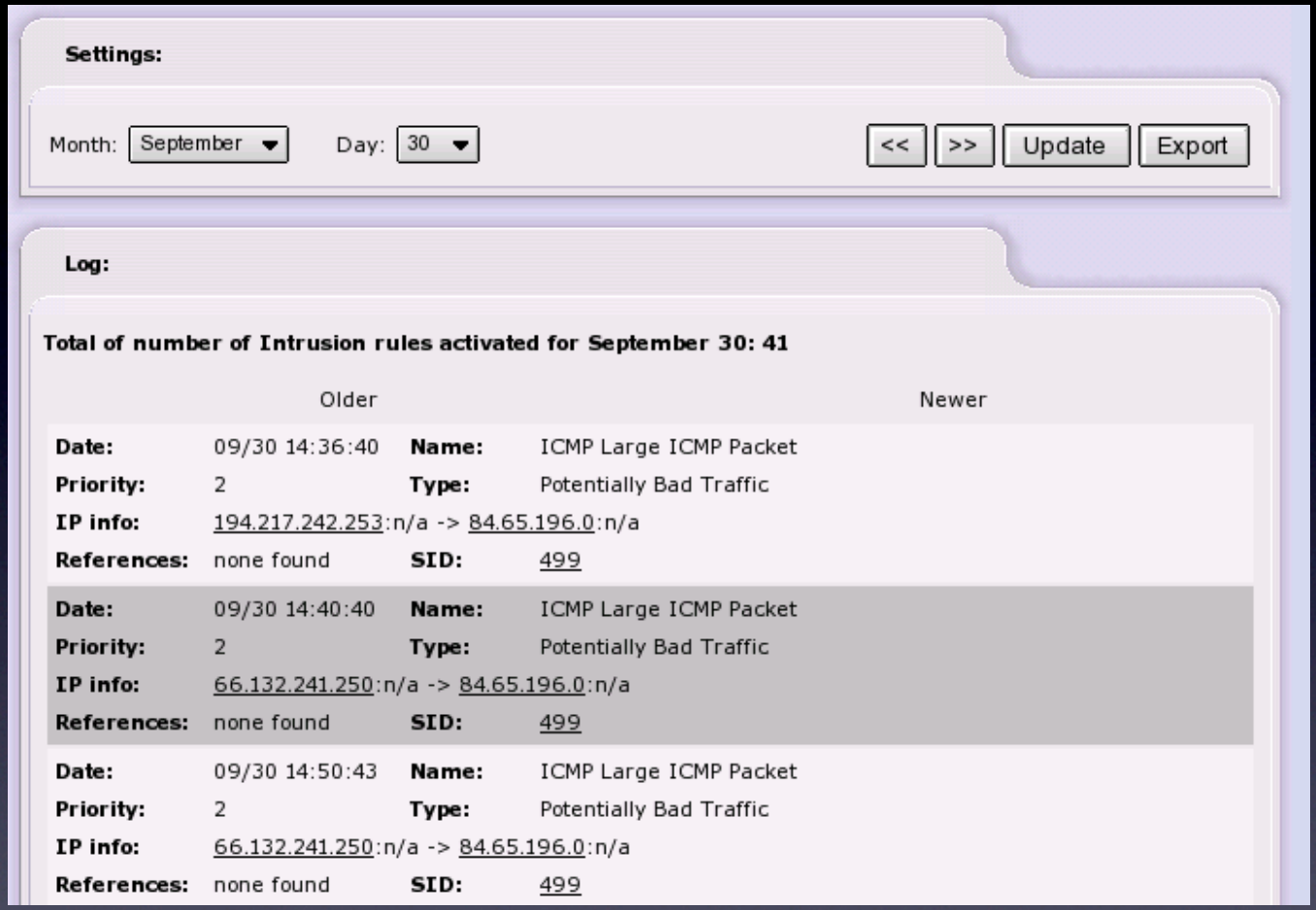
Data Leakage Prevention Event Data

Authentication Data

The History of Security Device Management


Log Viewer -- Security Log
File Edit View Filter Action Help
Time | Security Type | Severity | Direction | Protocol | Remote Host | Remote MAC | Local Host | Local MAC | Application Name
24/03/2009 20:26:40 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
24/03/2009 20:25:36 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
21/03/2009 22:18:52 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
21/03/2009 22:08:53 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
21/03/2009 22:07:47 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
20/03/2009 17:40:03 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
20/03/2009 17:29:50 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
20/03/2009 17:29:00 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
18/03/2009 13:53:16 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
18/03/2009 13:42:35 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
18/03/2009 13:42:12 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
17/03/2009 20:30:53 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
17/03/2009 20:20:10 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
17/03/2009 20:19:49 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
17/03/2009 11:33:06 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
17/03/2009 11:23:04 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
17/03/2009 11:22:01 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
15/03/2009 23:44:18 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
15/03/2009 23:34:14 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
15/03/2009 23:33:12 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
11/03/2009 08:13:30 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
11/03/2009 08:03:27 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
11/03/2009 08:02:26 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
10/03/2009 21:29:33 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
10/03/2009 21:19:32 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
10/03/2009 21:12:07 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
10/03/2009 21:10:19 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
10/03/2009 21:10:03 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
10/03/2009 20:31:51 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
10/03/2009 20:21:17 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
10/03/2009 20:20:45 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
10/03/2009 10:44:31 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
10/03/2009 10:34:28 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
10/03/2009 10:33:27 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
09/03/2009 18:49:46 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
09/03/2009 18:39:46 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
09/03/2009 18:39:40 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
09/03/2009 12:40:14 | Active Response Disengaged | Information | None | None | 61.139.105.163 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
09/03/2009 12:30:14 | Active Response | Major | Incoming | None | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
09/03/2009 12:29:11 | Port Scan | Minor | Incoming | TCP | 61.139.105.163 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
05/03/2009 11:30:40 | Active Response Disengaged | Information | None | None | 222.208.183.195 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
05/03/2009 11:20:39 | Active Response | Major | Incoming | None | 222.208.183.195 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
05/03/2009 11:19:38 | Port Scan | Minor | Incoming | TCP | 222.208.183.195 | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 |
04/03/2009 15:37:11 | Application Hijacking | Critical | Outgoing | TCP | www.winpatrol.com [161.58.14.137] | 00-06-2A-CA-A4-01 | | 00-C9-00-02-C4-E4 | C:\Program Files\BillP Studios\Wi
02/03/2009 00:39:04 | Active Response Disengaged | Information | None | None | 66.117.41.14 | 00-00-00-00-00-00 | | 00-00-00-00-00-00 |
02/03/2009 00:38:27 | Active Response Disengaged | Information | None | None | 66.117.41.18 | 00-00-00-00-00-00 | | 00-00-00-00-00-00
Traffic from IP address 61.139.105.163 is blocked from 03/24/2009 20:25:37 to 03/24/2009 20:35:37.

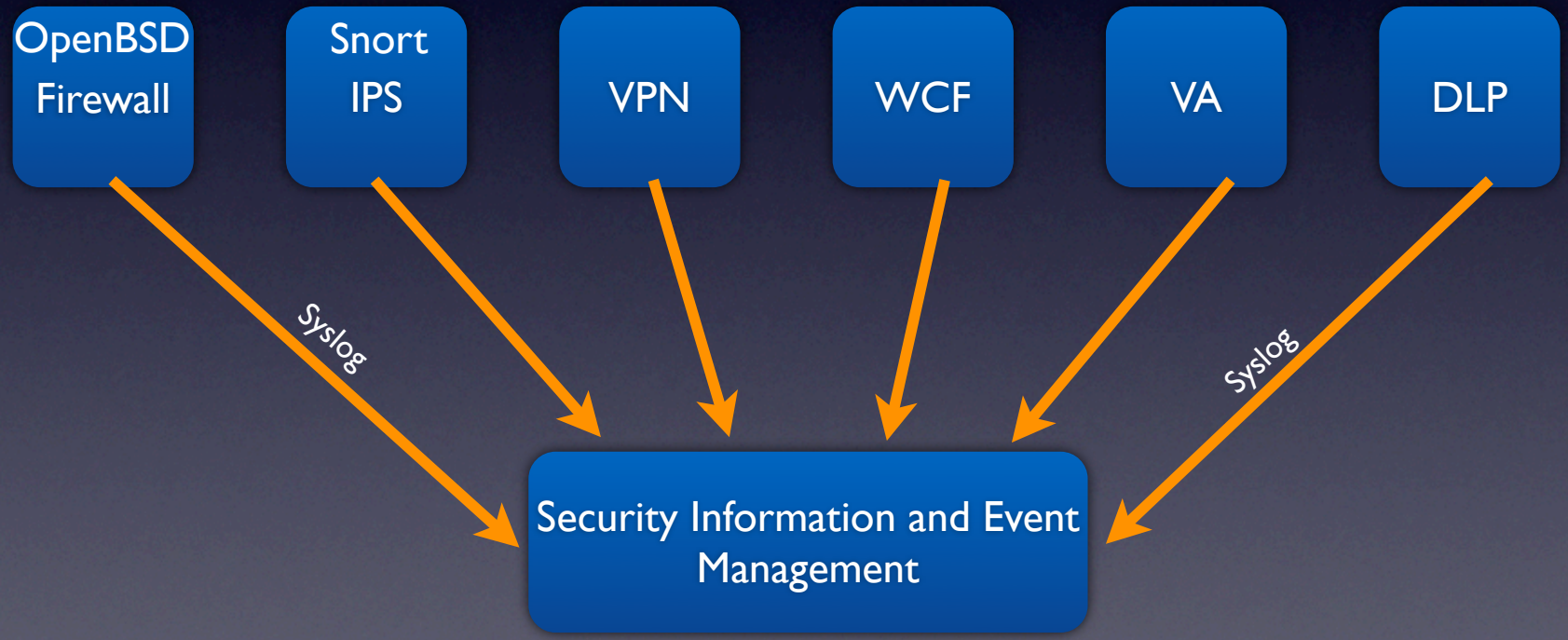
Firewall


Settings:
Month: September
Day: 30
<<
>>
Update
Export
Log:
Total of number of Intrusion rules activated for September 30: 41
Older
Newer
Date: 09/30 14:36:40 Name: ICMP Large ICMP Packet
Priority: 2 Type: Potentially Bad Traffic
IP info: 194.217.242.253:n/a -> 84.65.196.0:n/a
References: none found SID: 499
Date: 09/30 14:40:40 Name: ICMP Large ICMP Packet
Priority: 2 Type: Potentially Bad Traffic
IP info: 66.132.241.250:n/a -> 84.65.196.0:n/a
References: none found SID: 499
Date: 09/30 14:50:43 Name: ICMP Large ICMP Packet
Priority: 2 Type: Potentially Bad Traffic
IP info: 66.132.241.250:n/a -> 84.65.196.0:n/a
References: none found SID: 499

IPS

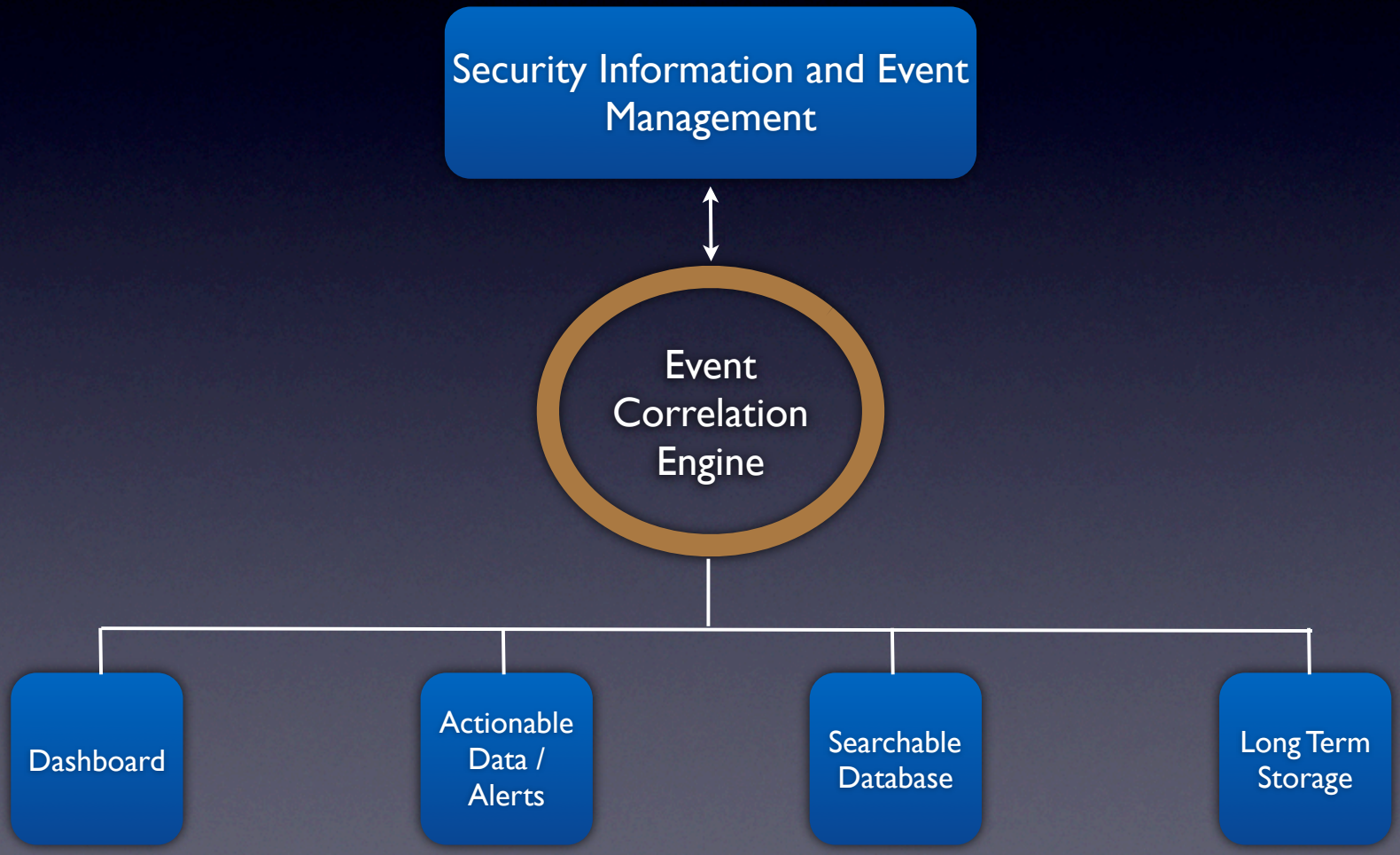
SIM, SEIM

SIM = Security Information Management



SIEM = Security Information and Event Management

Now What? (over simplified)



Dashboard

- View of Security Posture
- “At a Glance” Decision Points
- Configurable
- FAST Reporting at Admin’s Fingertips
- Compliance Friendly

Problem

- Data is Static
- Still Too Much
- Re-Actionable
- I want a BMW

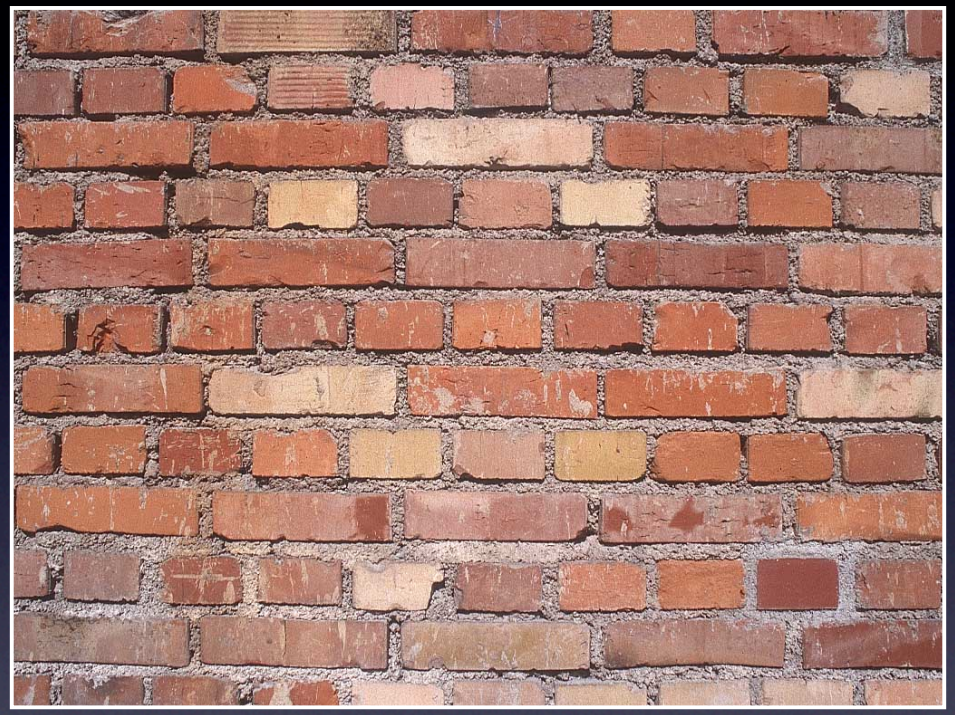
New Guys Doing Stuff

- Widget Based
- Faster Reporting
- Universal Interface
- Nice Guys

Steve Ocepek

Steve-O

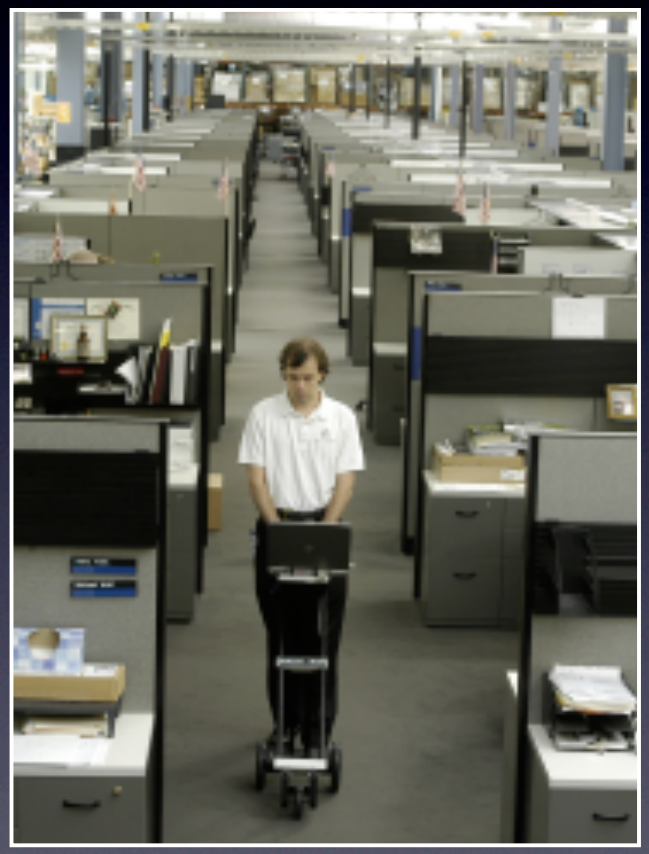
- Founded Wholepoint (early NAC)
- Four patents in network security
- Trustwave Senior Security Consultant (Pentesting) / CISSP
- Long-winded (turn on iPod now)



Where I came in

Internal Network Security

- De-perimeterization
- Rogue devices
- Wireless



Wholepoint

- Founded 2001
- 5 employees
- Angel investors

Wholepoint

- Founded 2001
- 5 employees
- Angel investors

Wp
WholePoint

Original Goals

- Know what's out there
- Ensure it's authorized
- If they're not.. KICK THEM OFF
  - YEAH!!

Differentiators

- Peer-based approach
- 3 patents granted
- Did I mention we kick people off your network?

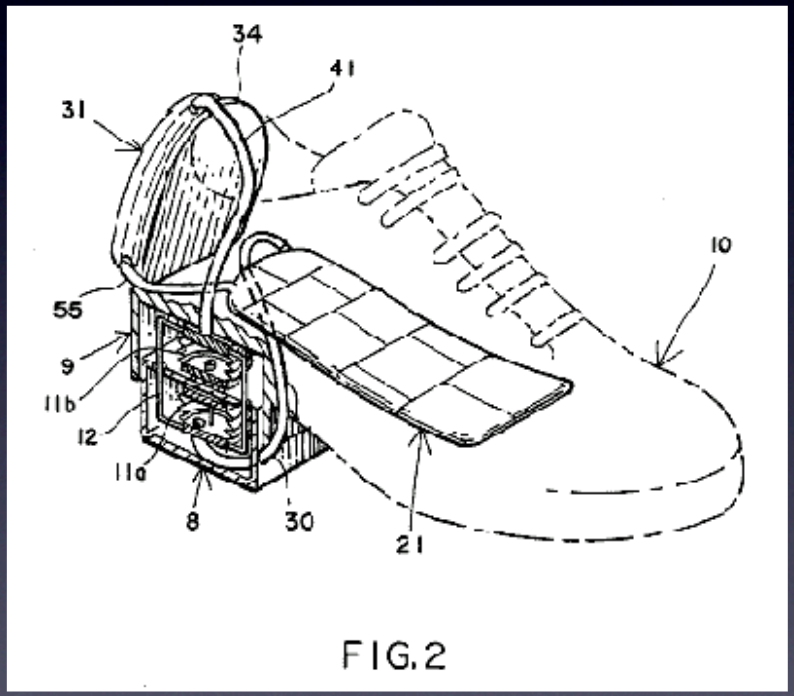


FIG. 2

But we were not alone

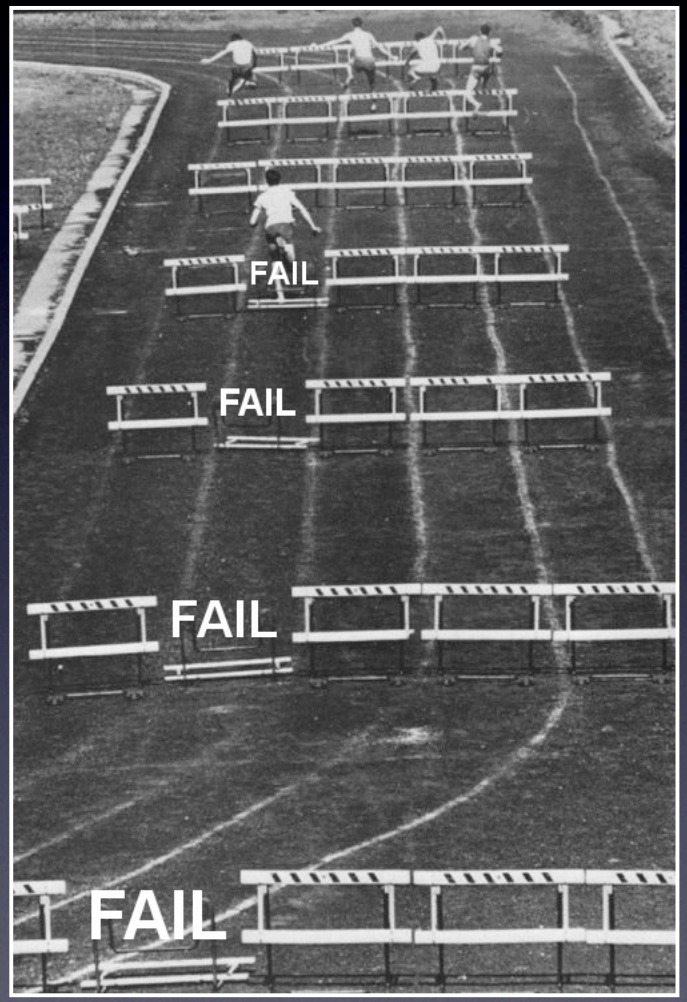
Getting up to speed

- 2004: Mirage purchases Wholepoint
- 2009: Trustwave purchases Mirage
- 2010: NAC "Where are they now?" is popular topic at RSA

What I have learned

Obstacles

- Workflow is different
- Lack of disruption tolerance
- Making good policy decisions is hard



The Problem

We don't understand our networks

Top Threats

- Unprotected Application Management Interfaces
- Unprotected Network Infrastructure Components
- Weak or No Credentials for Administrative Accounts

Source: Trustwave's Global Security Report, 2010

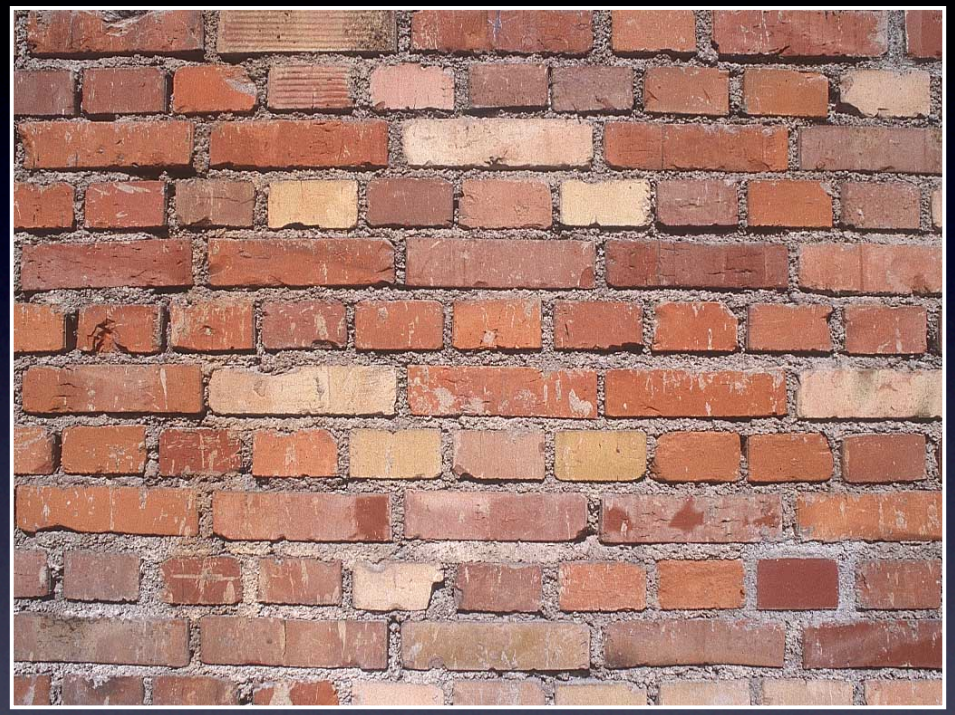
Security as a Multivitamin

- Consolidation of companies / technologies
- Bullet point selling
- Compliance checklists

False Positives

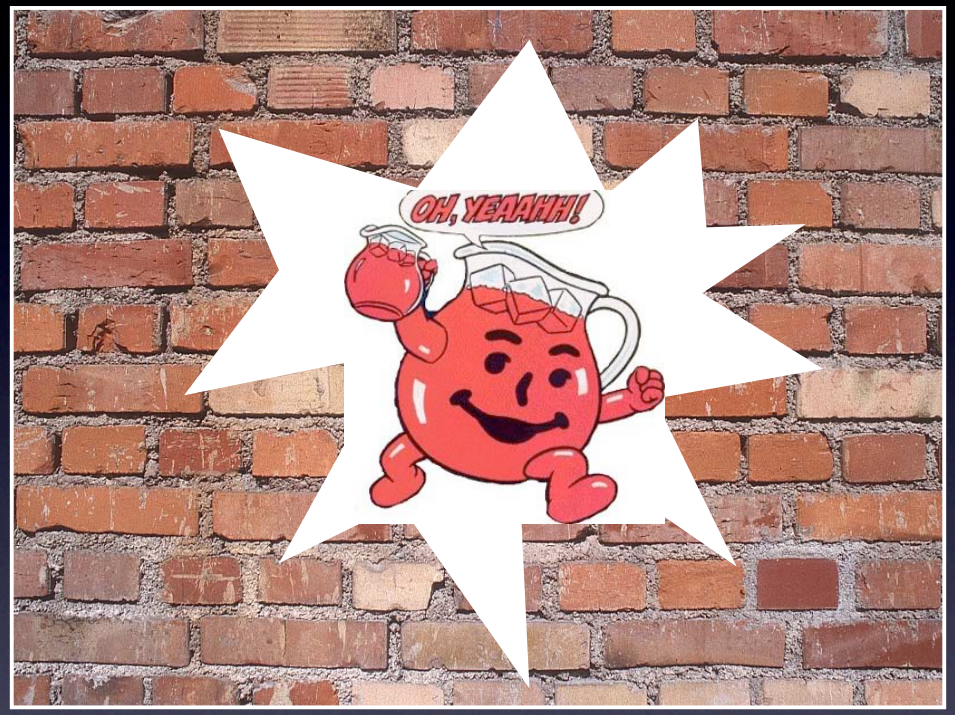
- Organizations want "tough" security
- Network admins don't have the time or the interest
- We have to make the decisions for them

That's how we got here



A Case for Visibility

The single most engaging aspect of security



A Case for Visibility

The single most engaging aspect of security

Q vs. A

Good security technology inspires good questions

Q vs. A

- Every network is different
  - Different systems in place
  - Different attitudes about security
  - Different needs
- One-size-fits-all cannot apply

Automatic Security

- "Security as a Product"
- Shields participants from details
- Offers good defaults to cover most popular cases

Visible Security

- Directly increases knowledge of all participants
- Ability to show and discuss data with peers
- Encourages (and requires) interaction with data set

Both are Needed

- Automatic Security is essential

  ... once we know what to tell it

- Visible Security fills in this gap

Visible Security Today

- Penetration testing
- Security Awareness Training
- Inventory systems
- Network monitoring tools
- NAC!

The Disconnect

- Focus continues to be on new automated systems
- Organizations have lost touch
- Reliance on compliance standards, hotfixes

Visible Networks

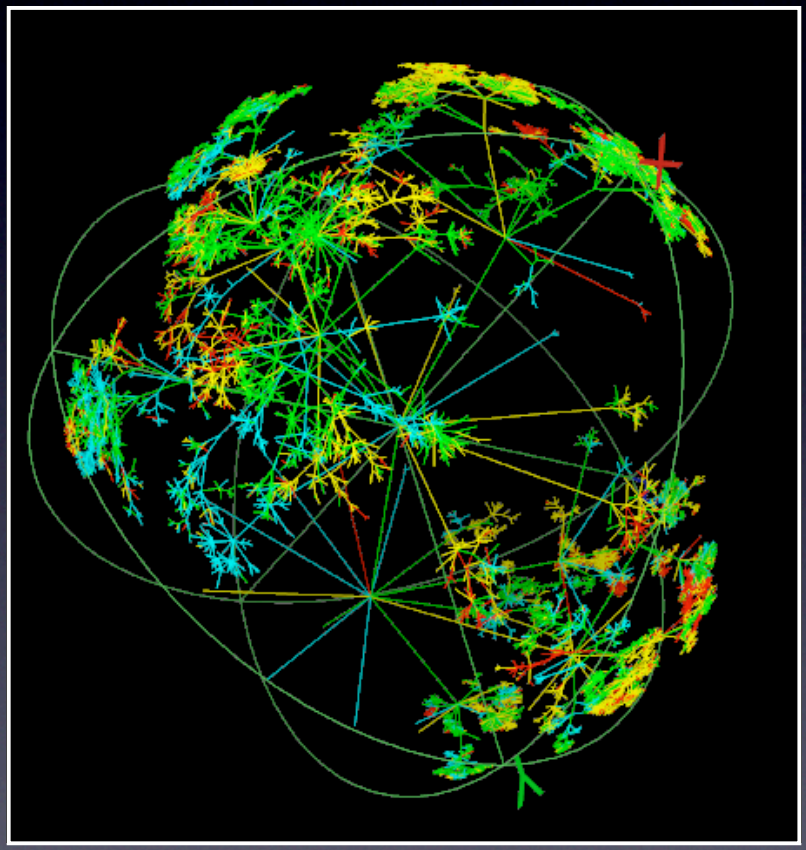
Observation

- Every network is different
- Networks are organic because *people* use them
- The local network is defined by *access* not by its *services*

Teaching systems to enforce network policy
without network visibility
is literally
the blind leading the blind

Challenges

- Need for meaningful results
- Dynamic, transient data
- Real-time, event-driven environment



Reality Check

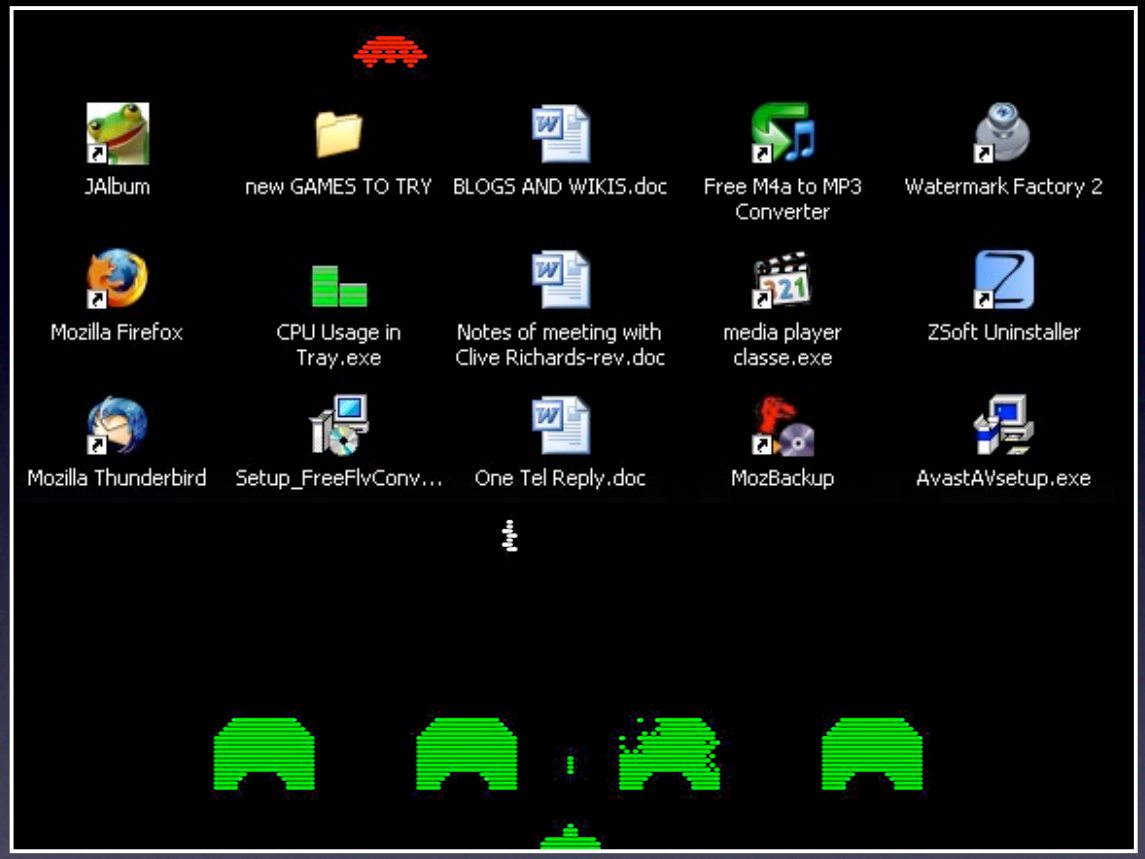
- This is lofty
- We need precedence
- Monitoring apps already exist, how does this differ?
- Who has faced similar challenges?
- How do we demonstrate this concept?

Playable Applications

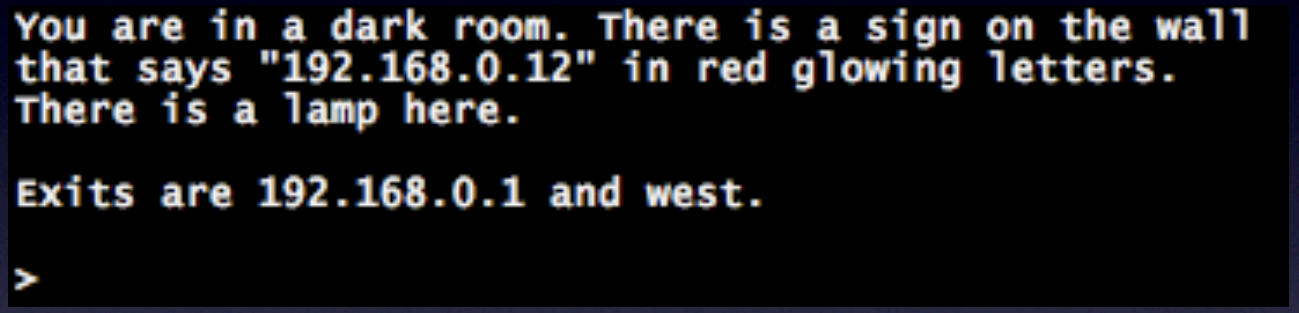
Do you like the buzzword? I made it myself.

Playable Apps

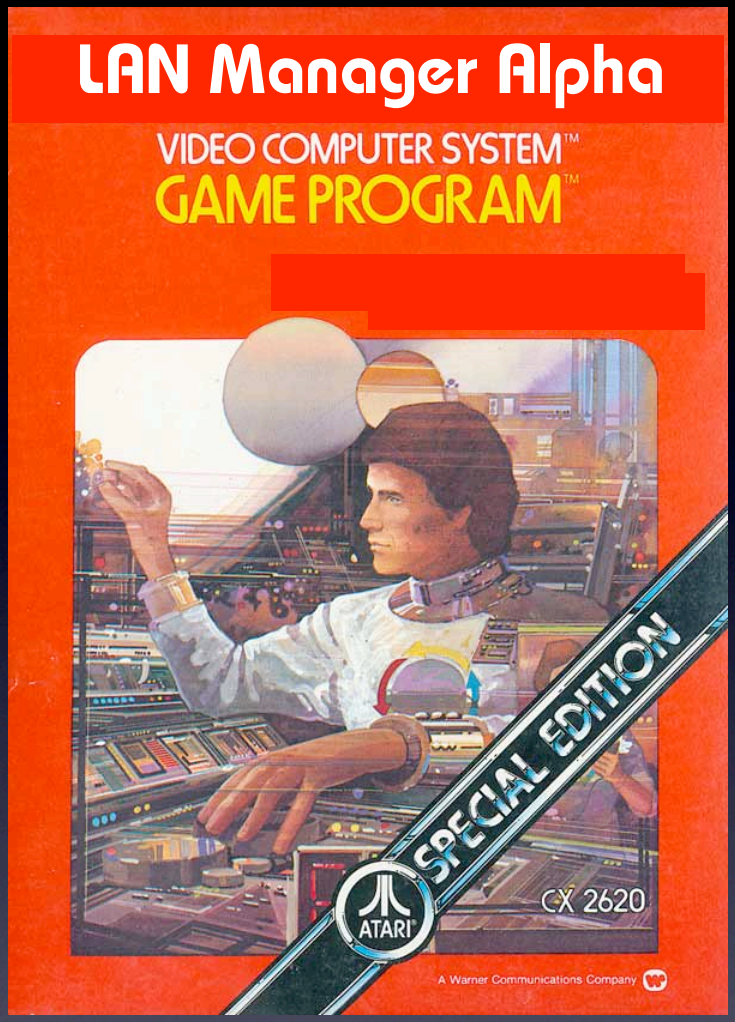
- Game design applied to applications
- Heavily focused on user experience
- Presentation, Communication, Abstraction are key components



What this is not



What this is not



What this is not

What this is

- An opportunity to tap into design methodologies that:
  - Drive a multi-billion dollar industry
  - Effectively teach non-technical users complex tasks
  - Facilitate group communication and cooperation

Prediction

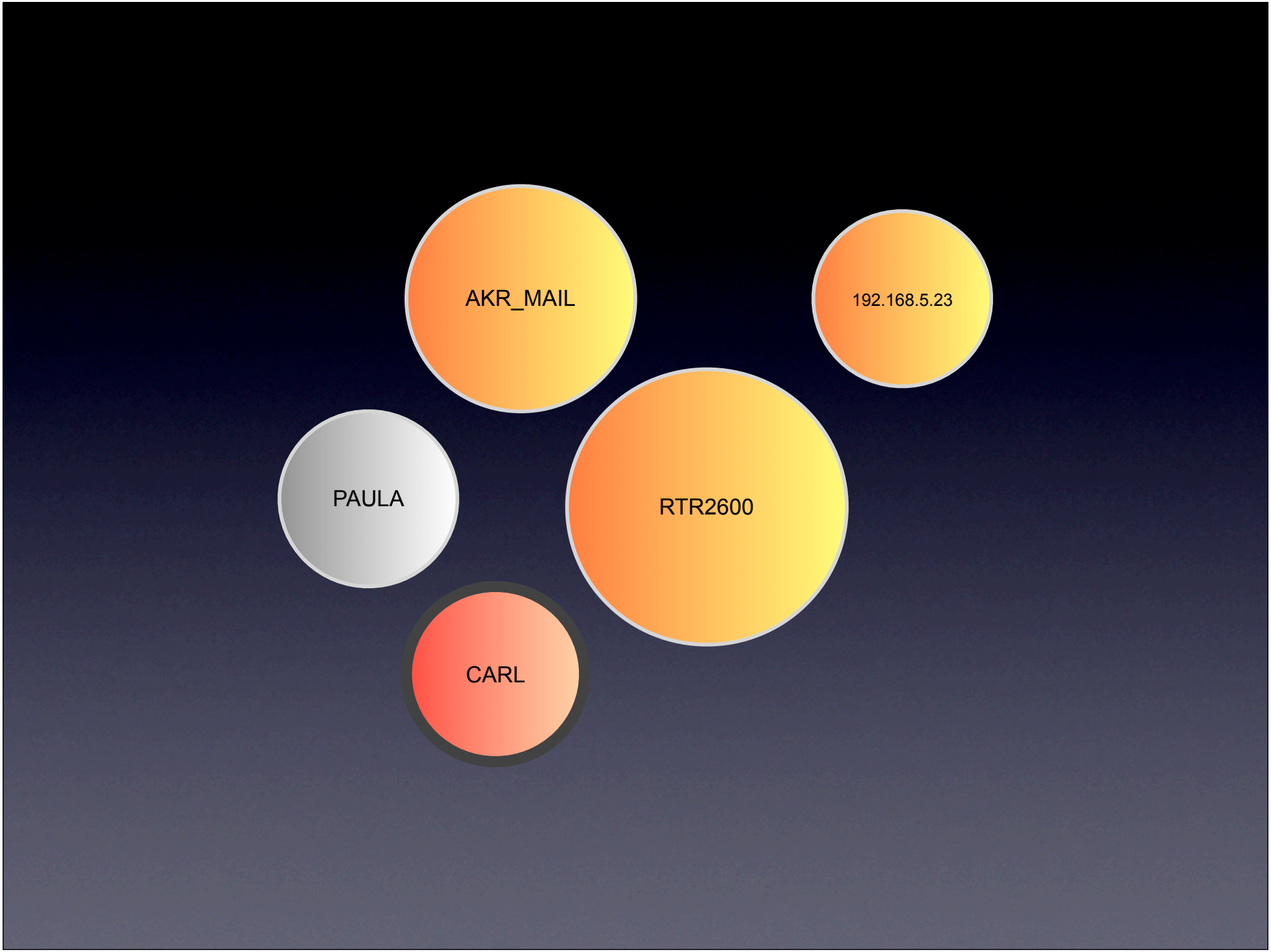
Playable network security will raise awareness and result in more effective solutions

Concepts

- Presentation
- Communication
- Abstraction

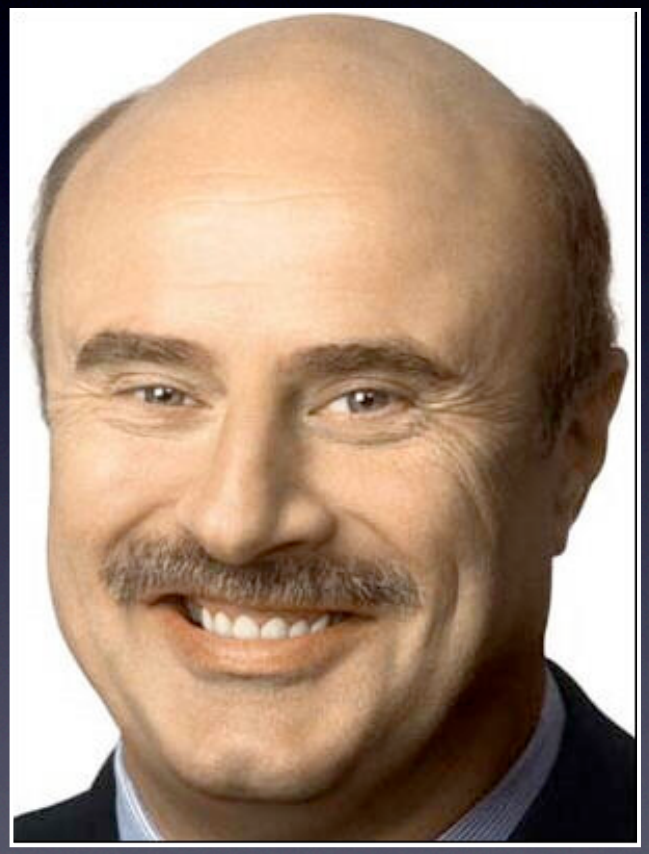
Presentation

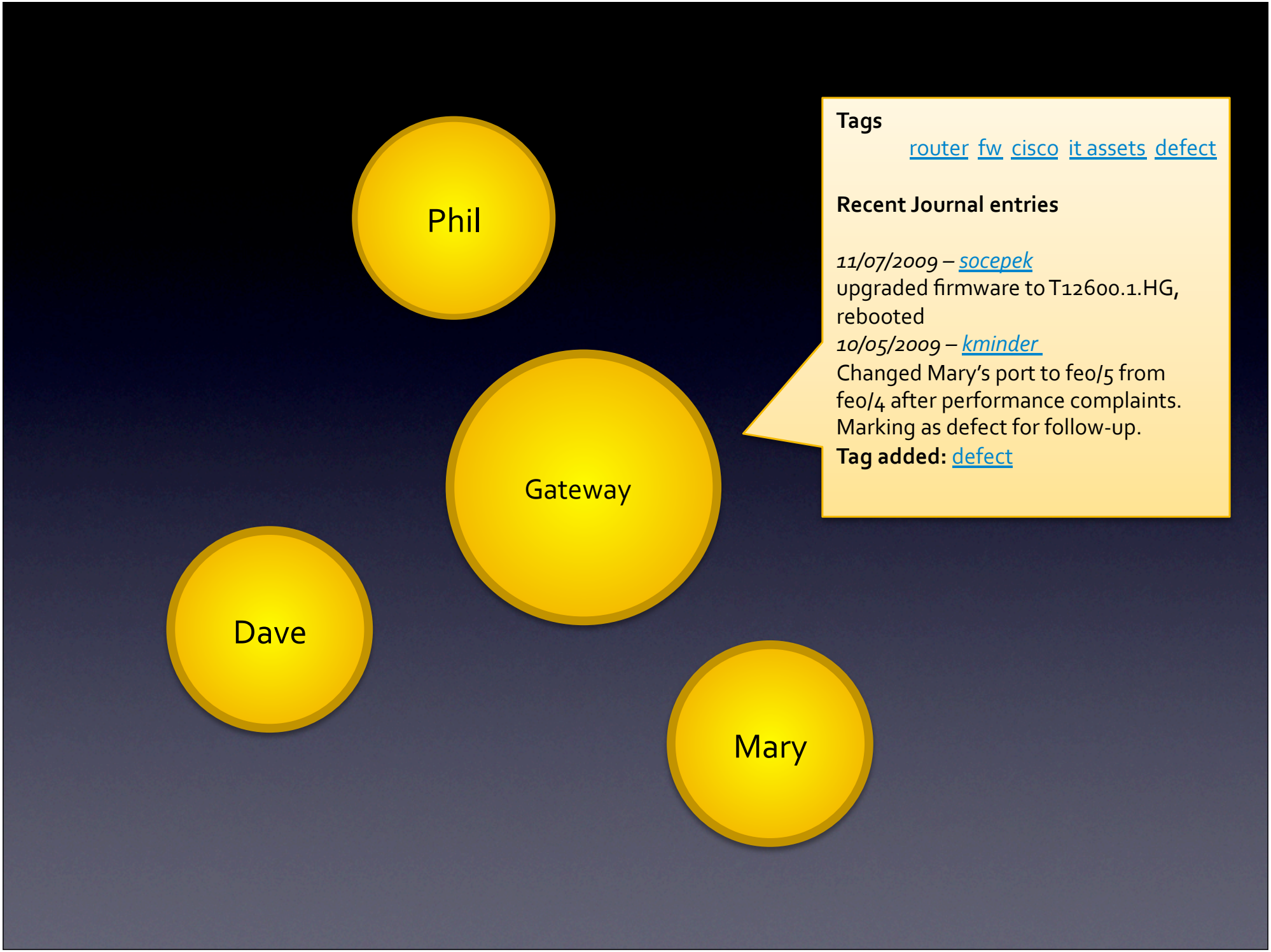
- Making the application engaging and appealing
- Adjectives like “polished”, “robust”, “intuitive”
- Apple is incredibly good at this


AKR_MAIL
192.168.5.23
PAULA
RTR2600
CARL

Communication

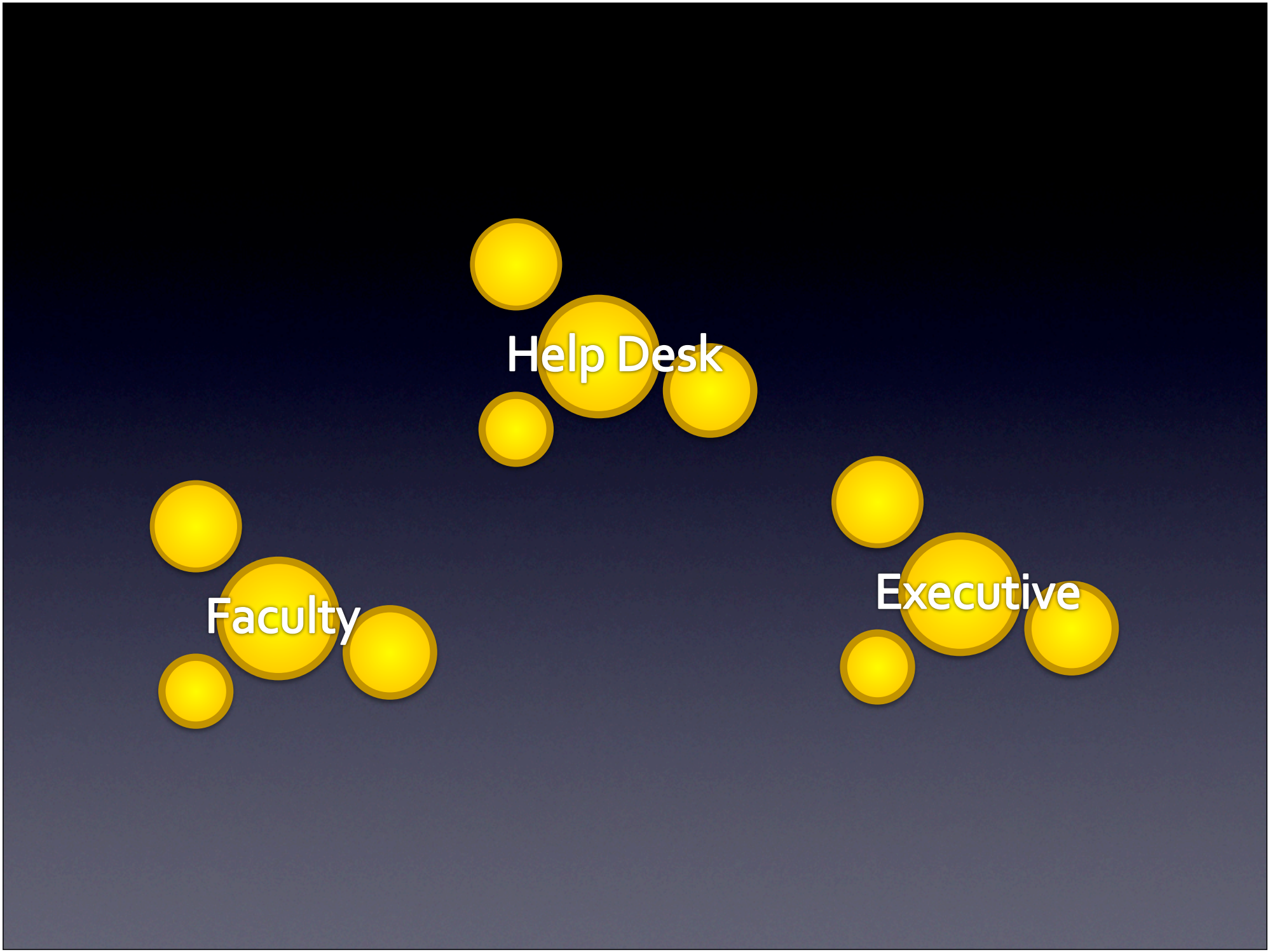
- Multi-user design methodology
- Goal is to keep the user "in-app"
- Users see each other online, can chat and share data




Phil
Gateway
Dave
Mary
Tags
router fw cisco it assets defect
Recent Journal entries
11/07/2009 – socepek
upgraded firmware to T12600.1.HG, rebooted
10/05/2009 – kminder
Changed Mary's port to fe0/5 from fe0/4 after performance complaints. Marking as defect for follow-up.
Tag added: defect

Abstraction

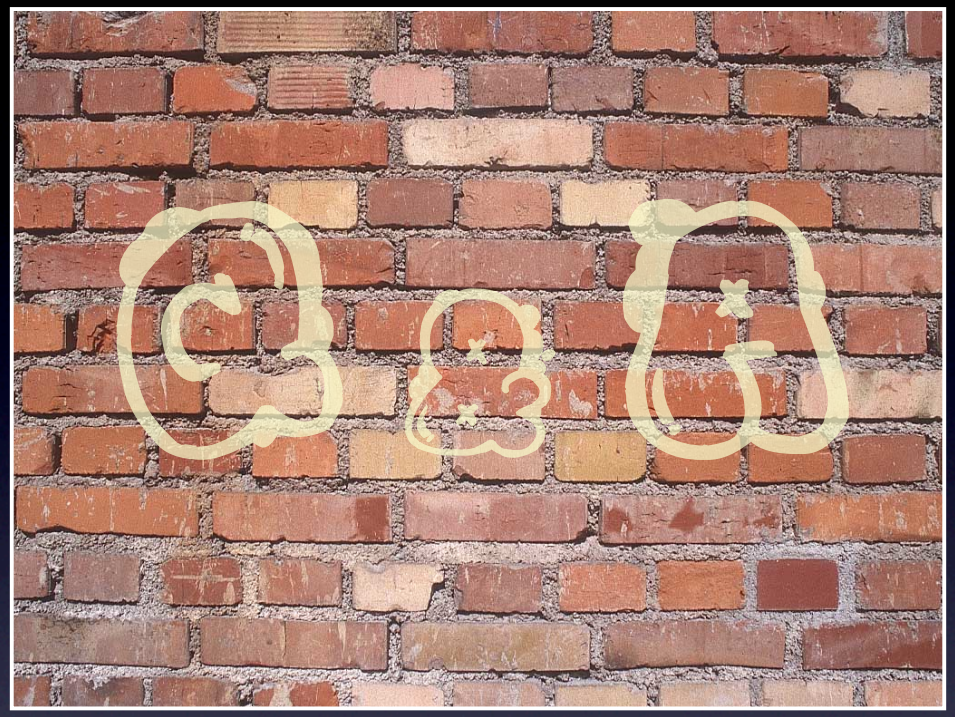
- But how does it scale?
- Key element of game design
- Missing ingredient in most monitoring applications
- “Humanizes” the dataset


Help Desk
Faculty
Executive

Conclusion

I need an excuse for my video game habit

questions@kurtisminder.com



Kurtis E Minder CISSP
kurtis@kurtisminder.com

Steven Ocepek CISSP
socepek@fastmail.net