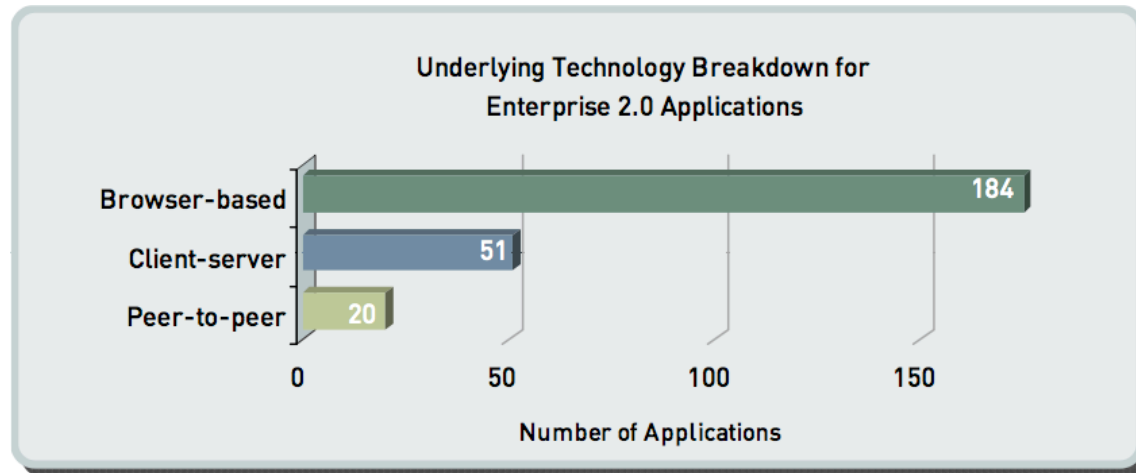


# Assessing Risk to the Network Introduced by Web 2.0 Applications



# About the report

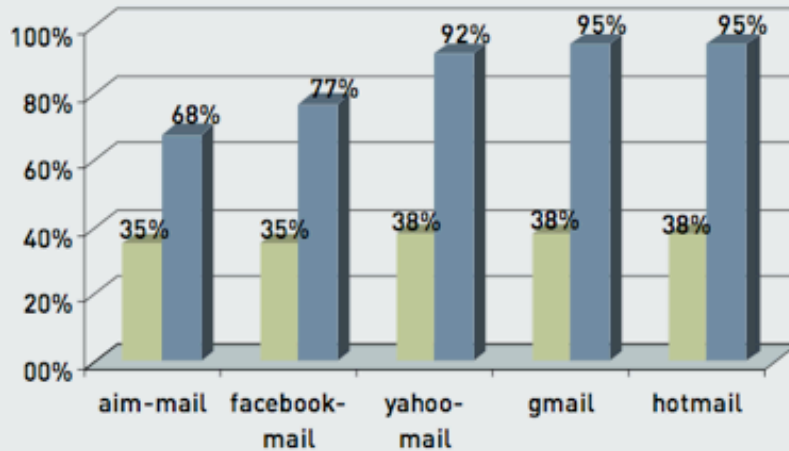
- Global view of assessments between March and September 2009:
  - 1,000,000+ people
  - 214 organizations
  - 651 observed applications
- Comparisons data between Spring/Fall 2009



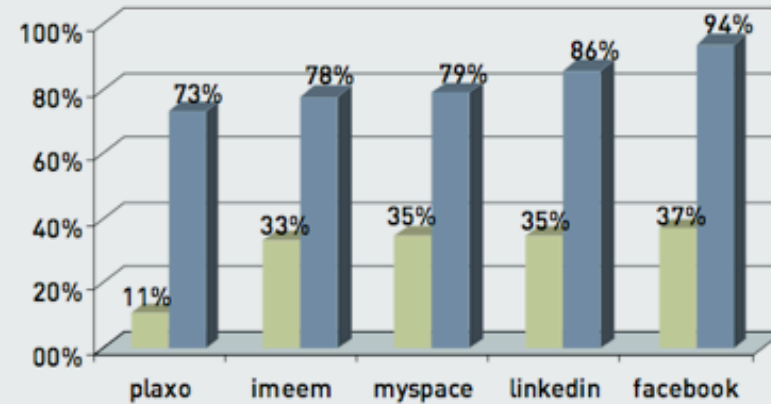
One Problem!

# Application Adoption is Exploding

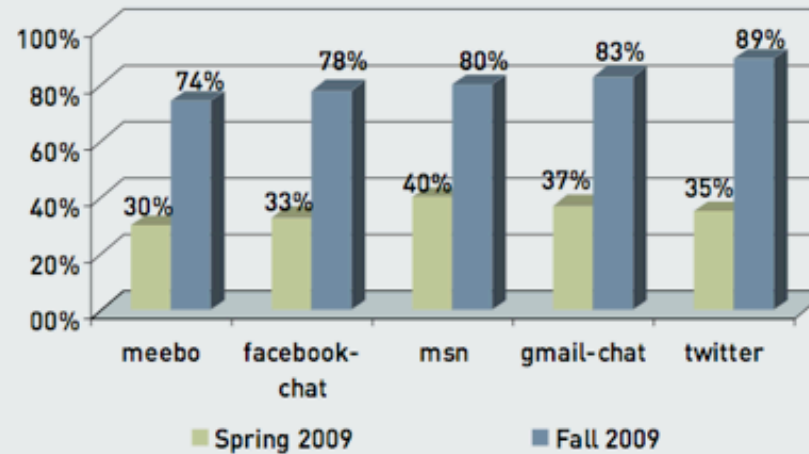
### Growth in Webmail Applications



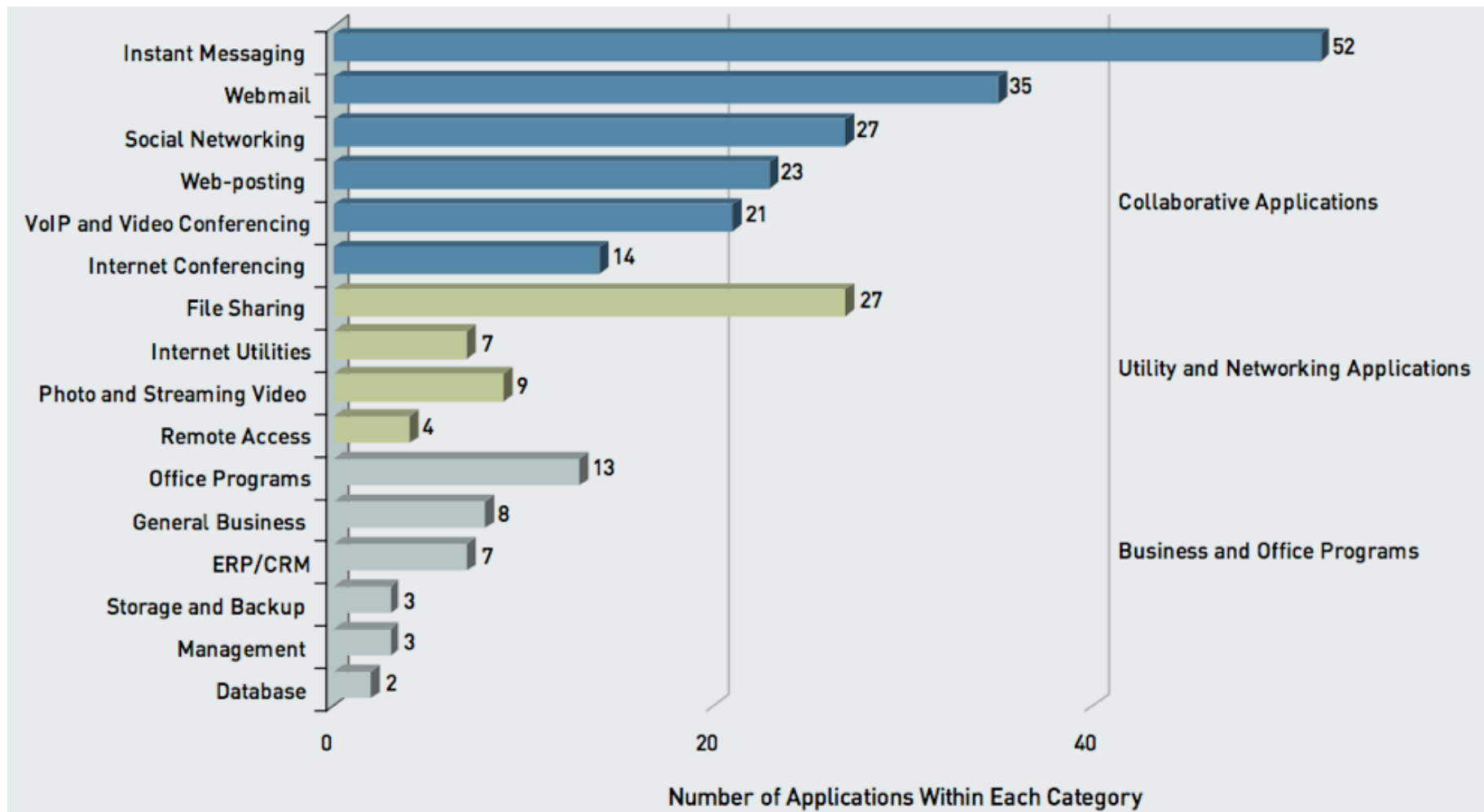
### Growth in Social Networking Applications



### Growth in Instant Messaging Applications

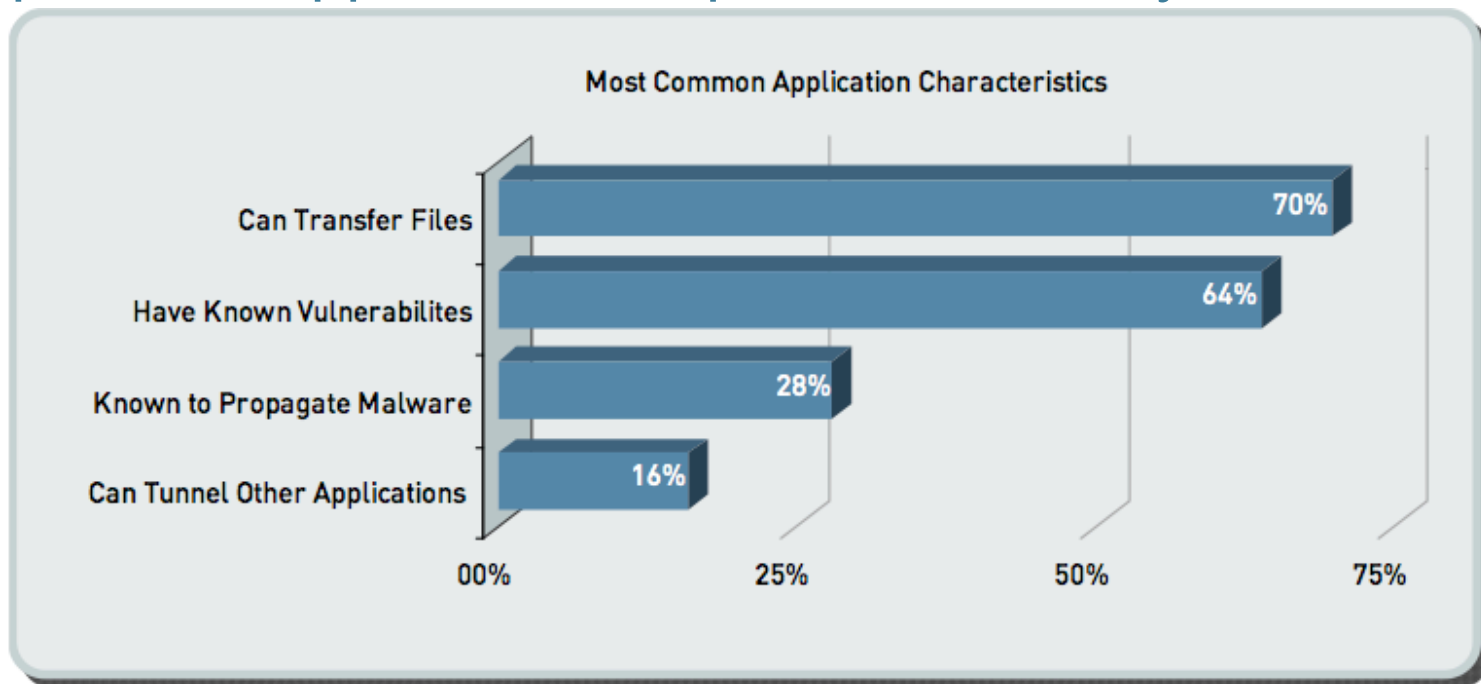


# Enterprise 2.0 Application Category Breakdown



# Applications are not Threats, but...

- The same applications used for social interaction are being used for work-related purposes.
- 72% of traffic sampled is browser based.
- Enterprise 2.0 application adoption is driven by users, not by IT.



# Applications can be Threats

- Most significant risk is leakage/loss of personal and corporate data due to file transfer capabilities (70%) within the application.
- Applications with known vulnerabilities (64%) can propagate threats.
- Applications can be used by malware (28%).
- Social networking users are a “target rich” environment.
- New threats due to implied trust of social networking:
  - Koobface
  - Fbaction
  - Boface

Click Now - Think Later

# Key Application Concerns

- External proxies.
- Hiding applications in encrypted tunnels.
- Remote desktop control applications.
- P2P file sharing usage is rampant.
- Browser-base file sharing is gaining in popularity.
- Entertainment consumes enormous bandwidth.
  - 78% at universities, over 50% on average
- Applications are designed for accessibility (port hopping, port 80, port 443).
- Port 80 does not have to mean web traffic.

## 5 things to know about Microsoft SharePoint

- SharePoint showed up in 91% of the enterprises analyzed in the two most recent Palo Alto Networks risk reports.
- According to Neil McDonald of Gartner, 30% of SharePoint deployments are rogues.
- SharePoint uses IIS and MS-SQL - which introduces business and security risks targeting IIS and SQL.
- In these same two reports, 38 instances of critical, high and medium severity threats targeting MS SQL, IIS and SharePoint were found.
- 17 fold increase in bandwidth consumed and 4 fold increase in session consumption per organization.

# Things to know about Twitter

- Twitter is being used heavily.
- The most popular instant messaging application (89%), up from 35% in Spring 2009.
- 252% increase in sessions consumed for Twitter (more frequent periods of use).
- Bandwidth consumed increased 775%, even with 140 characters, average was 184 MB per organization.

# Things to know about FaceBook

- Detected in 94% of organizations.
- Bandwidth jumped 294% to 6.3 GB per organization.
- Sessions increased by 192%.
- Facebook Mail and Chat have become the 4th most commonly detected applications.
- In a mere 18 months, it has become more widely used than Yahoo! IM and AIM (within this sample).
- Are your employees farmers or mobsters?

# Games: Farmers and Mobsters



## App Leaderboard

	Name	MAU
1.	FarmVille	83,105,118
2.	Birthday Cards	47,272,535
3.	Static FBML	36,019,145
4.	Café World	30,547,447
5.	Facebook for iPhone	28,225,238
6.	Texas HoldEm Poker	27,211,570
7.	Happy Aquarium	26,131,260
8.	Mafia Wars	25,080,678
9.	iHeart	24,914,444
10.	Causes	24,267,597
11.	FishVille	24,245,704
12.	Slide FunSpace	22,985,995
13.	Zoo World	20,334,974
14.	MindJolt Games	19,782,786
15.	PetVille	19,567,573
16.	Pet Society	19,157,781
17.	Friends Exposed	18,185,877
18.	Mobile	18,063,069
19.	Friend Quiz	17,317,628
20.	FamilyLink.com	15,439,952
21.	Restaurant City	14,855,917

MAU - Monthly Active Users

## P2P - Peer to Peer

- An average of six P2P variants were found in 9 out of 10 organizations.
- In one extreme case, 17 P2P variants were found.
- The most common P2P were BitTorrent and Gnutella.
- Industry leaks: Laura Bush's safe house, detailed list of a civilian nuclear complex, Marine One blueprints and healthcare records.
- P2P consumed 22% of total bandwidth in university networks.
- P2P is shifting to browser-based file sharing
  - Examples: RapidShare & Skydrive

# Why isn't P2P being blocked?

- Employees use whatever applications they want.
- Enterprise networks are often faster than home networks.
- “Free” stuff: music, videos, software, etc.
- P2P applications are evasive:
  - Port hopping
  - Masquerading as HTTP
  - Proprietary encryption to avoid detection
    - For example: uTorrent
- URL filtering cannot block P2P traffic.

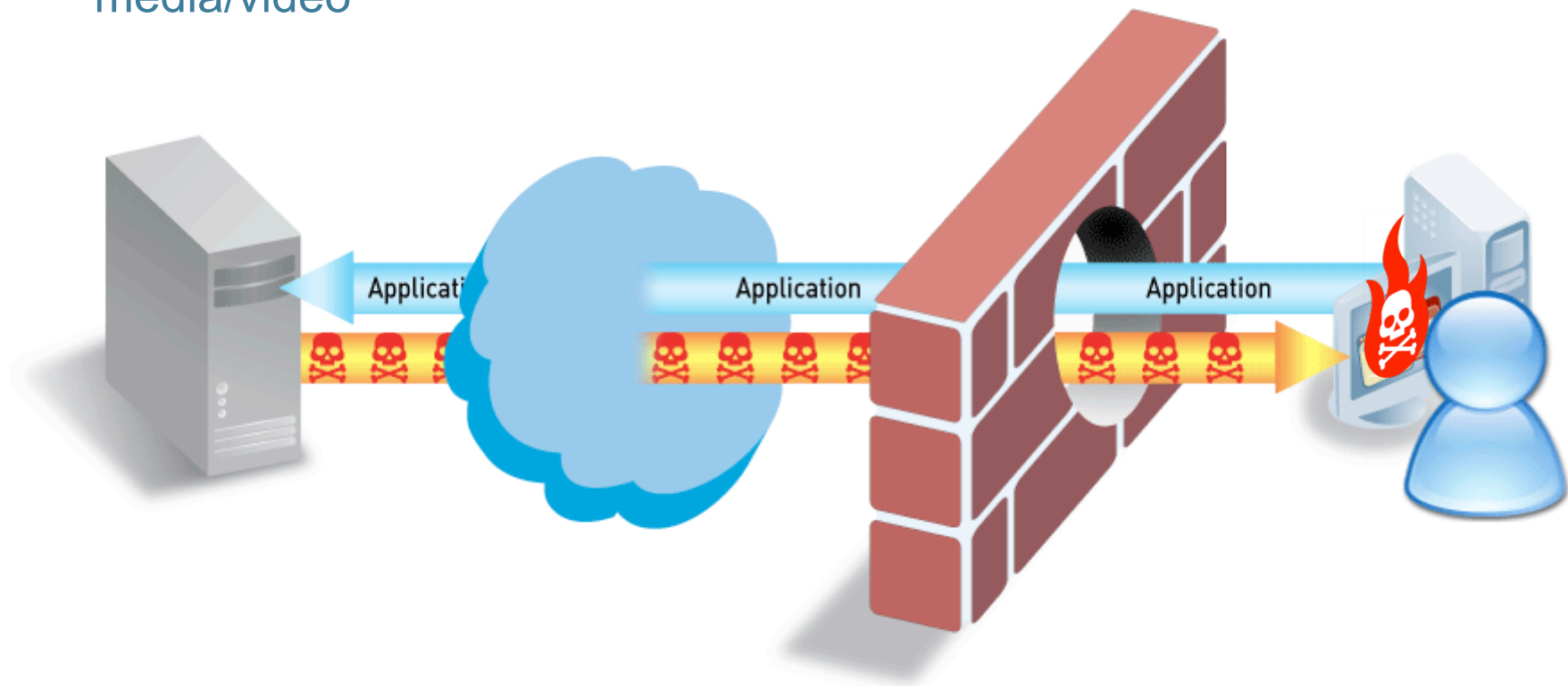
# Applications Carry Risk

## Applications can be “threats”

- P2P file sharing, tunneling applications, anonymizers, media/video

## Applications carry threats

- SANS Top 20 Threats – majority are application-level threats



Applications & application-level threats result in major breaches – Pfizer, VA, US Army

# Application Chaos Increases Business Risks

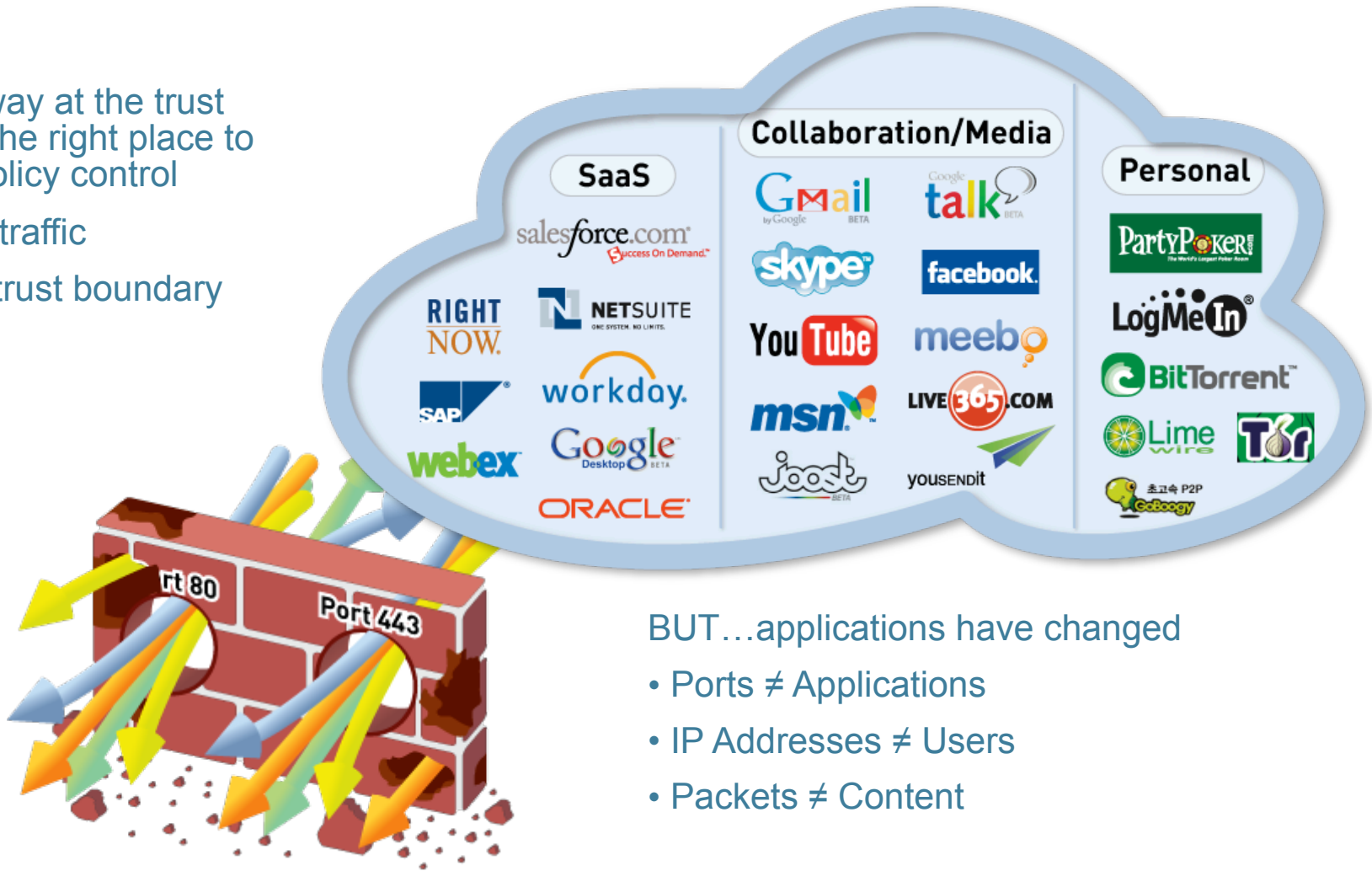
- Data loss: Unauthorized or unmonitored employee file transfer, hacker imposed data breach.
- Non-compliance: Employees using unapproved applications – IM in financial and healthcare services.
- Operational cost overruns: Excessive bandwidth consumption, desktop cleanup.
- Employee productivity loss: Excessive personal application usage – media, streaming audio, social networking, webmail, IM, file sharing.
- Business continuity: Malware or application vulnerability induced downtime.

Employees can access any application they want and at any time!

# Applications Have Changed; Firewalls Have Not

The gateway at the trust border is the right place to enforce policy control

- Sees all traffic
- Defines trust boundary

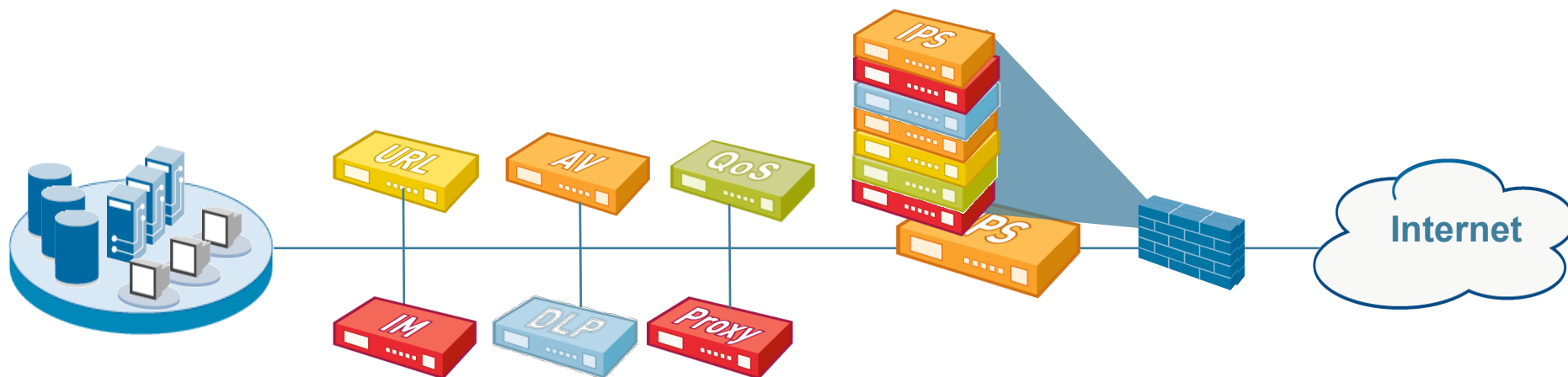


BUT...applications have changed

- Ports  $\neq$  Applications
- IP Addresses  $\neq$  Users
- Packets  $\neq$  Content

Need to restore visibility and control in the firewall

# Technology Sprawl & Creep Are Not The Answer



- “More stuff” doesn’t solve the problem
- Firewall “helpers” have limited view of traffic
- Complex and costly to buy and maintain
- Putting all of this in the same box is just slow

# It's Time to Fix the Firewall!

## New Requirements for the Firewall

1. Identify applications regardless of port, protocol, evasive tactic or SSL
2. Identify users regardless of IP address
3. Granular visibility and policy control over application access / functionality
4. Scan application content in real-time (prevent threats and confidential data leaks)
5. Multi-gigabit, in-line deployment with no performance degradation



# Speakers & Contacts

- Altaware, Inc., Werner Schmidt
  - <http://www.altaware.com>
  - [wschmidt@altaware.com](mailto:wschmidt@altaware.com)
  - 949-468-0020 x101
- Palo Alto Networks, Mary Farrelly and Santiago Polo
  - <http://www.paloaltonetworks.com>
  - [mfarrelly@paloaltonetworks.com](mailto:mfarrelly@paloaltonetworks.com)
  - 310-376-6608

# Application Visibility Report

What's running on **your** network?

Request a network analysis:

[AVR-request@altaware.com](mailto:AVR-request@altaware.com)

