What's Next for the Next Generation Firewall Vendor Palo Alto Networks Overview

October 2010

Matias Cuba - Regional Sales Manager
Northern Europe

paloalto NETWORKS

the network security company™

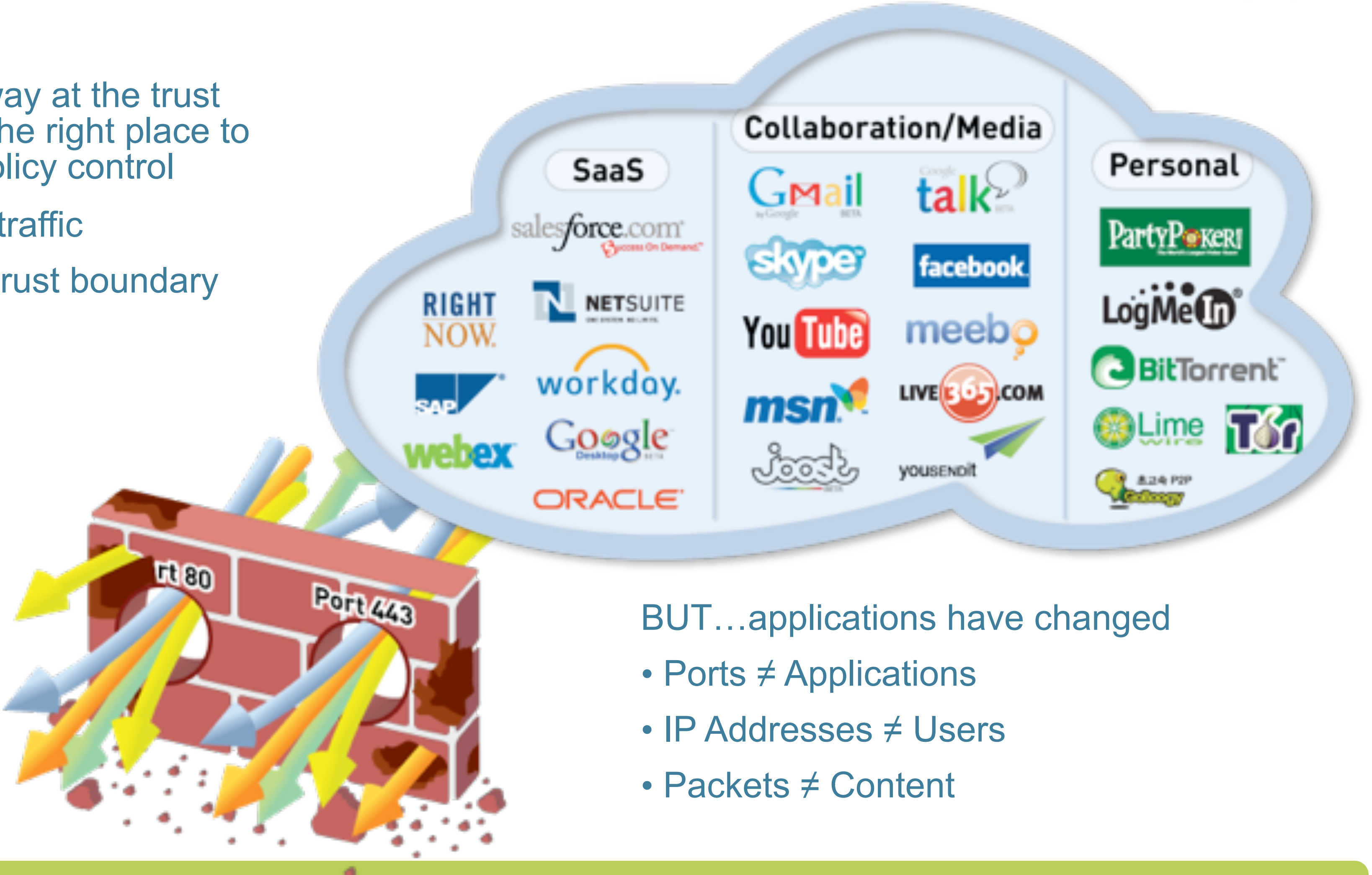
About Palo Alto Networks

- Palo Alto Networks is the **Network Security Company**
- World-class team with strong security and networking experience
  - Founded in 2005 by security visionary Nir Zuk
  - Top-tier investors
- Builds next-generation firewalls that identify / control 1000+ applications
  - Restores the firewall as the core of the enterprise network security infrastructure
  - Innovations: App-ID™, User-ID™, Content-ID™
- Global footprint: 2,000+ customers in 50+ countries, 24/7 support

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 ≠ Applications
- IP Addresses ≠ Users
- Packets ≠ Content

Need to restore visibility and control in the firewall

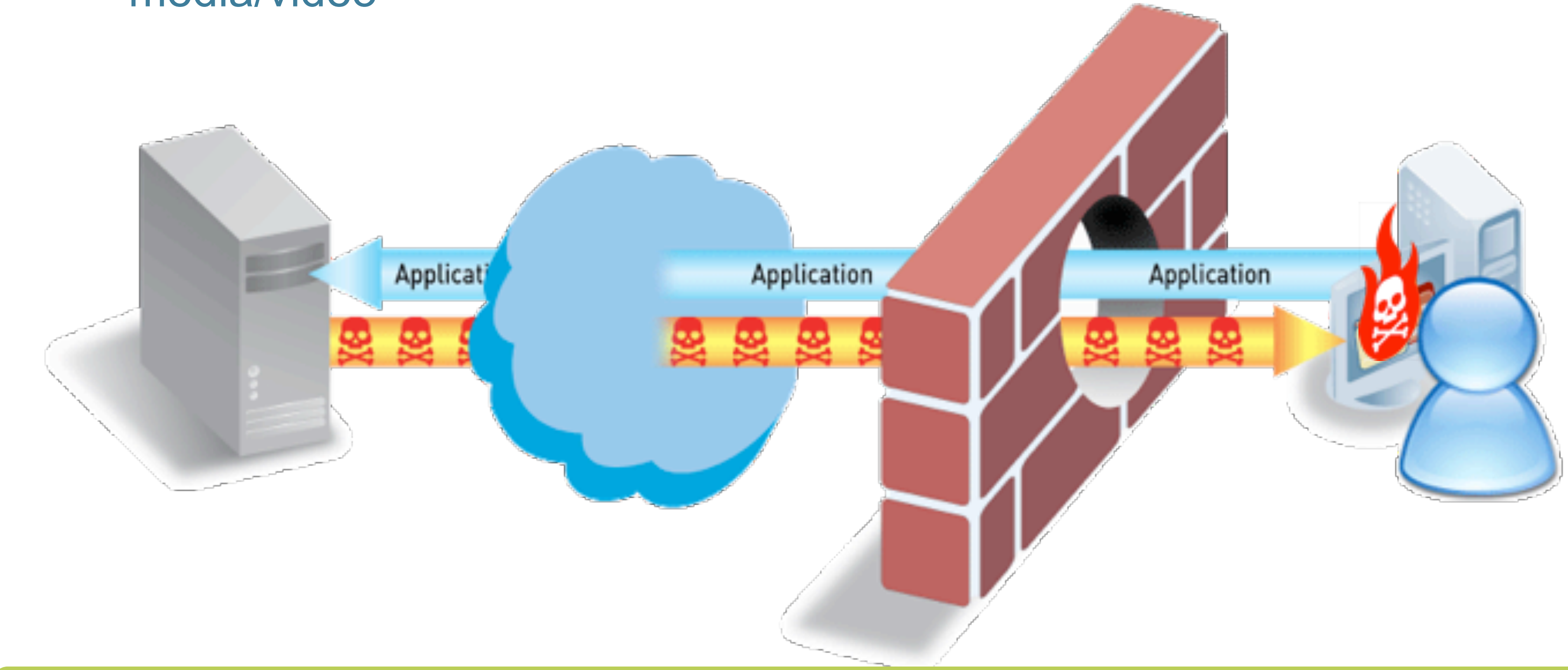
Applications Carry Risk

Applications can be “threats”

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

Applications carry threats

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

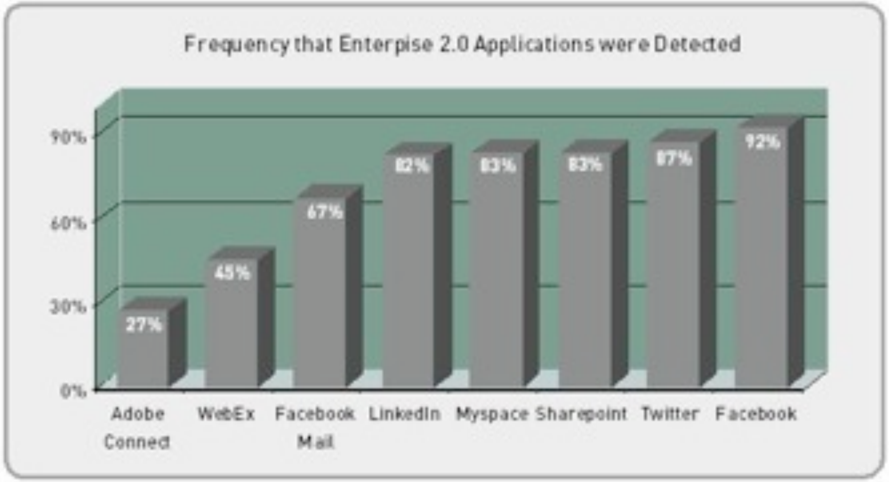


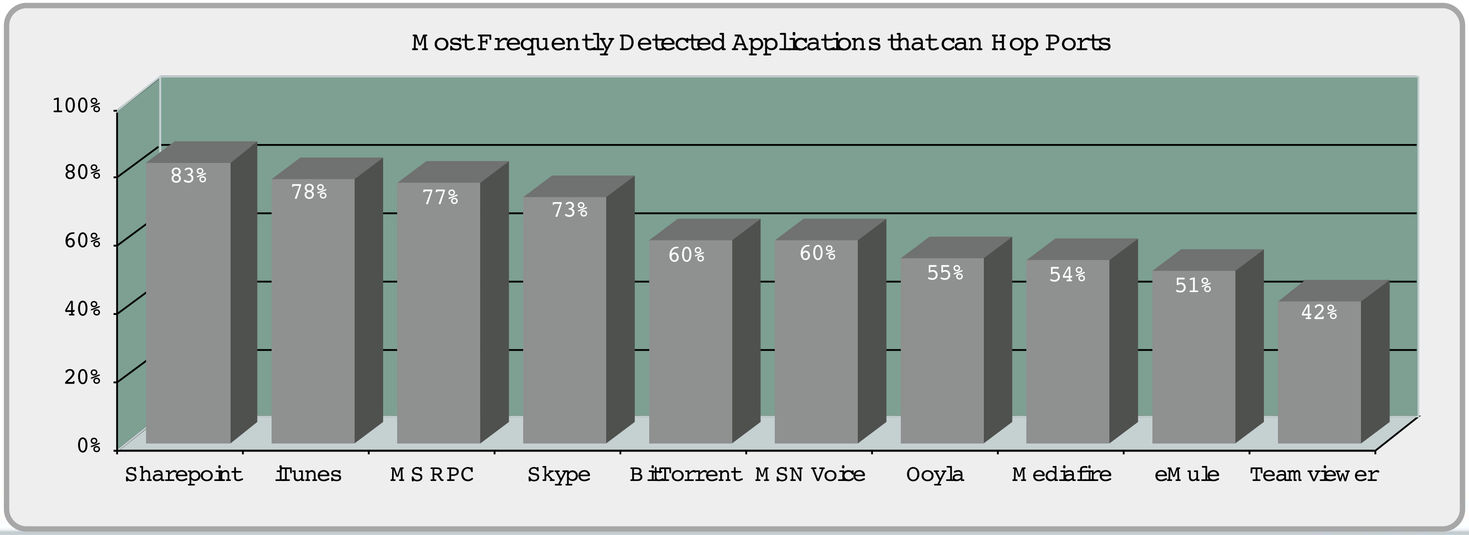
Applications & application-level threats result in major breaches – Pfizer, VA, US Army

Enterprise 2.0 Applications and Risks Widespread

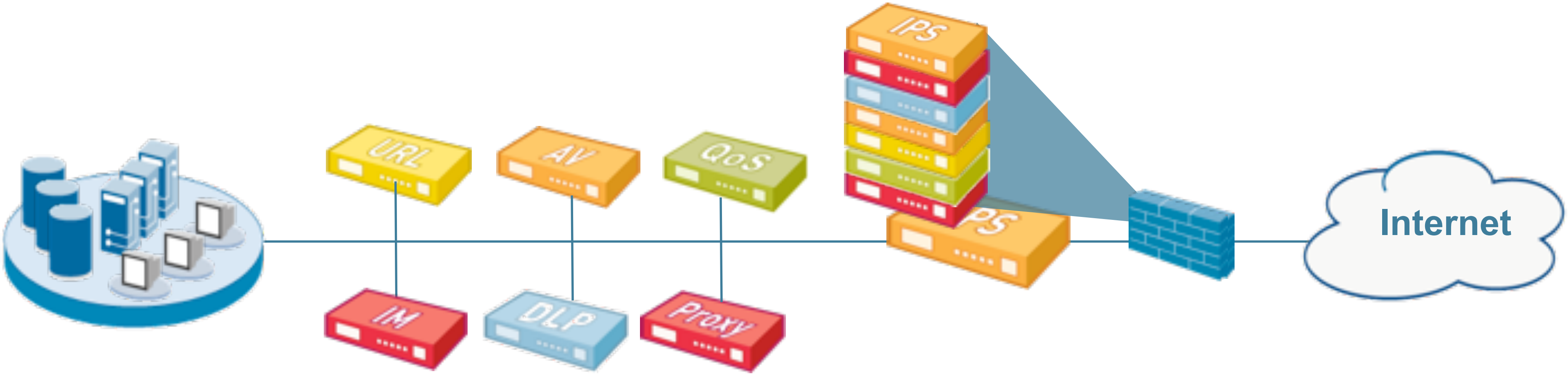
Palo Alto Networks' latest Application Usage & Risk Report highlights actual behavior of 1M+ users across more than 340 organizations

- Enterprise 2.0 applications – like Twitter, Facebook, and Sharepoint – continue to rise for both personal and business use. Facebook and Google extend dominance outside of core applications
- Tunneling and port hopping are common
- Bottom line: all had firewalls, and most had IPS, proxies, & URL filtering – but none of these organizations could control what applications ran on their networks





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

The Right Answer: Make the Firewall Do Its Job

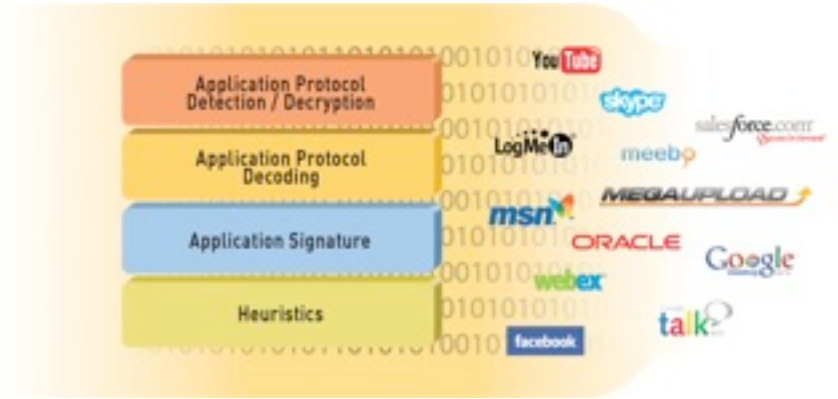
New Requirements for the Firewall

1. Identify applications regardless of port, protocol, evasive tactic or SSL
2. Identify users regardless of IP address
3. Protect in real-time against threats embedded across applications
4. Fine-grained visibility and policy control over application access / functionality
5. Multi-gigabit, in-line deployment with no performance degradation

Identification Technologies Transform the Firewall

App-ID™

Identify the application


Application Protocol Detection / Decryption

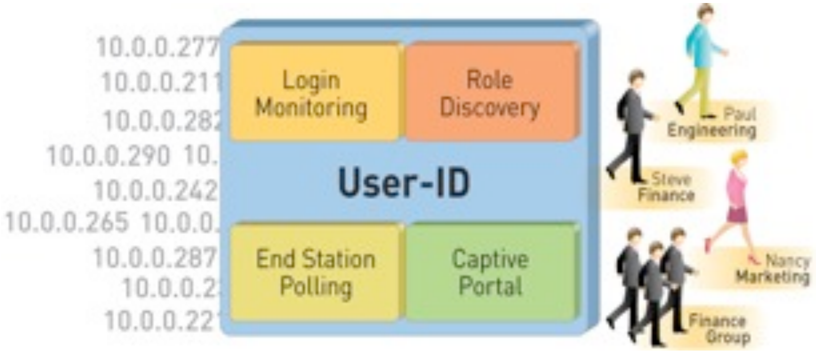
Application Protocol Decoding

Application Signature

Heuristics

User-ID™

Identify the user


Login Monitoring

Role Discovery

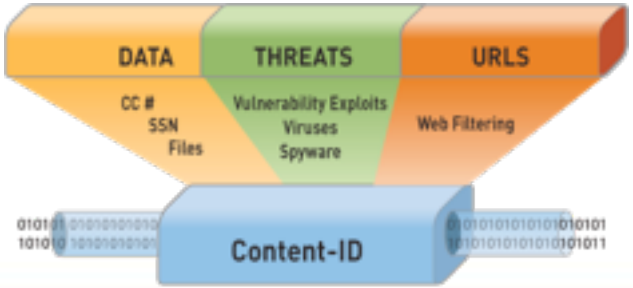
User-ID

End Station Polling

Captive Portal

Content-ID™

Scan the content


DATA

THREATS

URLS

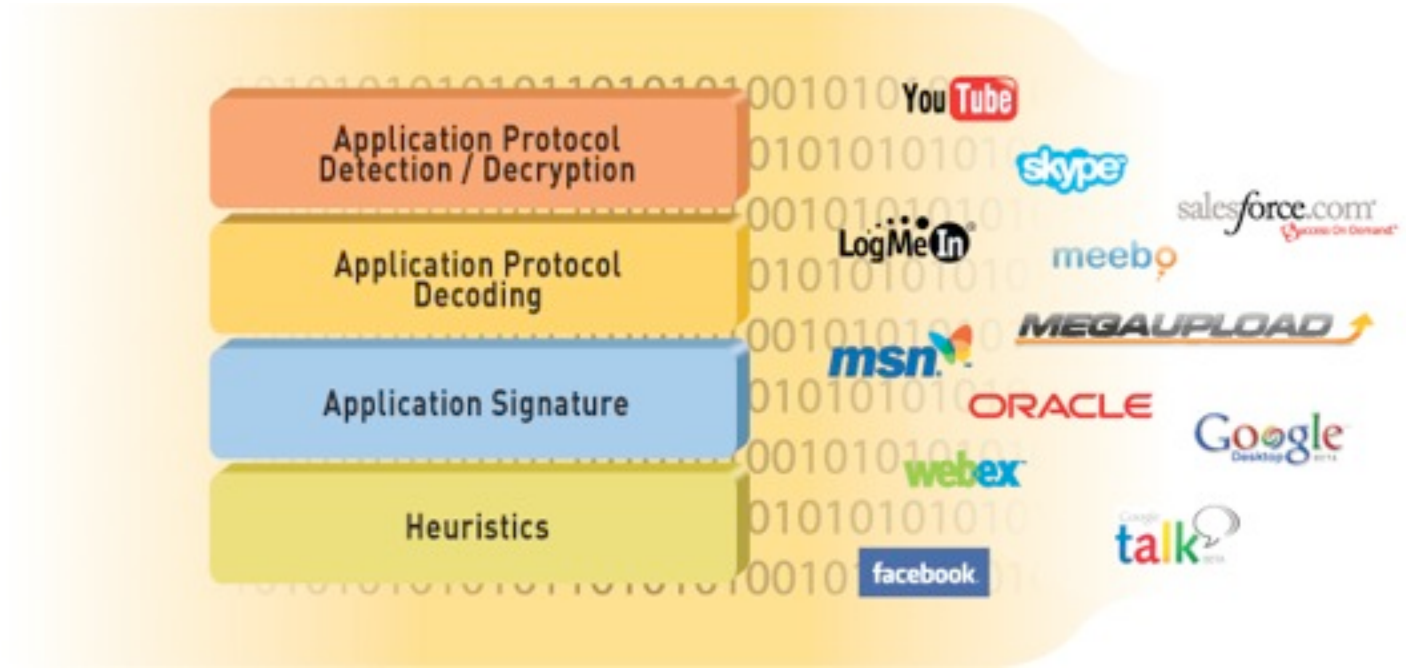
CC #
SSN
Files

Vulnerability Exploits
Viruses
Spyware

Web Filtering

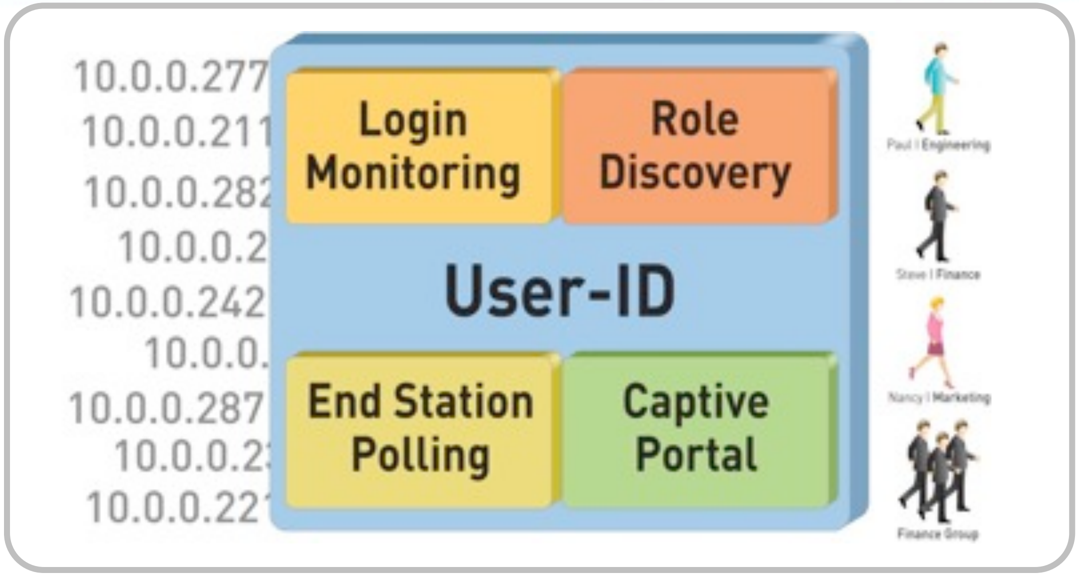
Content-ID

App-ID: Comprehensive Application Visibility



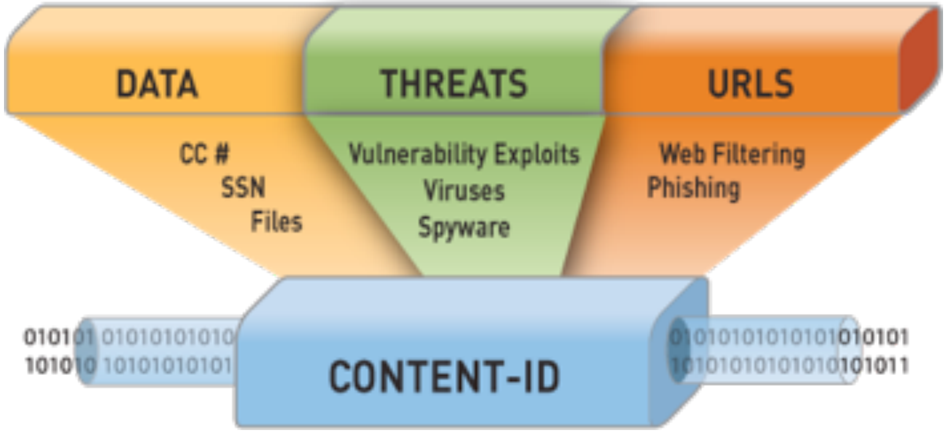
- Policy-based control more than 1000+ applications distributed across five categories and 24 sub-categories
- Balanced mix of business, internet and networking applications and networking protocols
- Custom applications can be added easily

User-ID: Enterprise Directory Integration



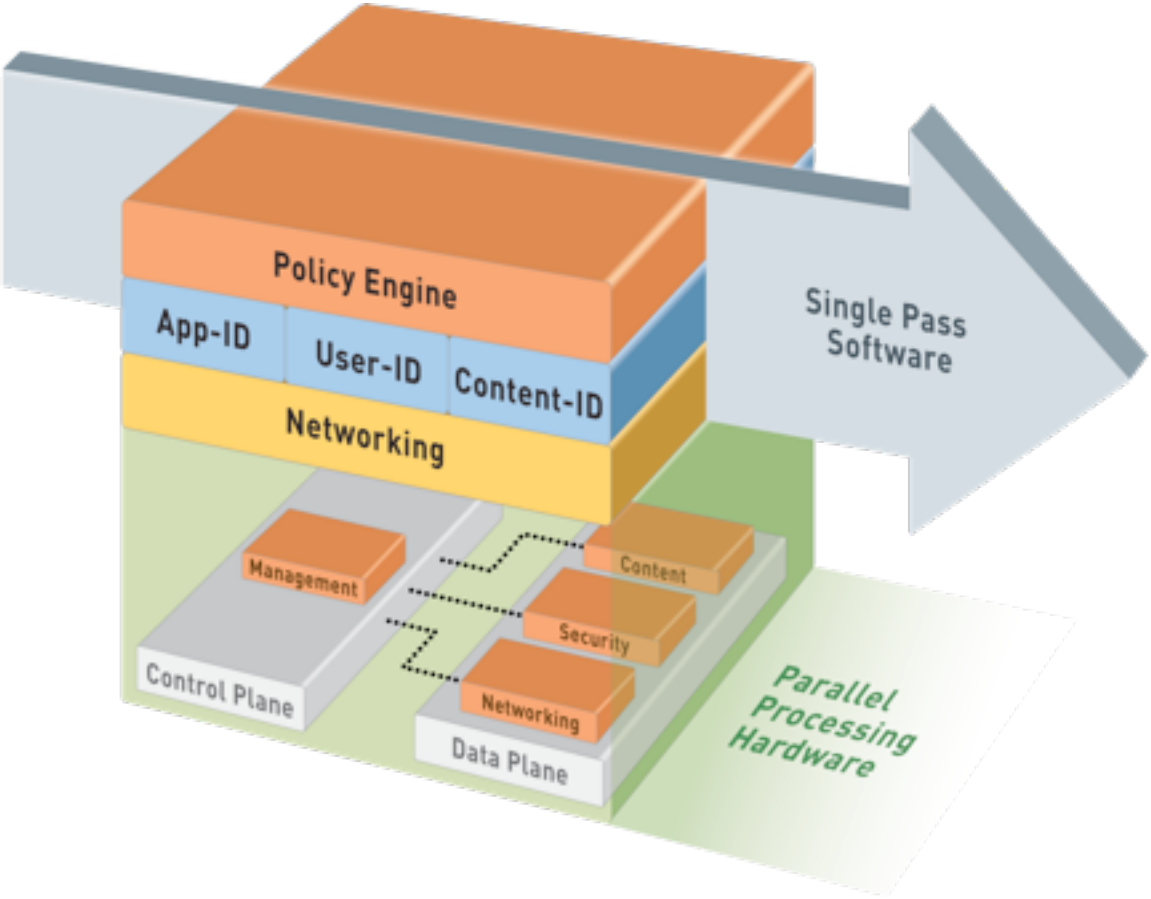
- Users no longer defined solely by IP address
  - Leverage existing Active Directory infrastructure
- Understand users application and threat behavior based on actual AD username, not just IP
- Manage and enforce policy based on user and/or AD group
- Investigate security incidents, generate custom reports

Content-ID: Real-Time Content Scanning



- Detect and block a wide range of threats, scan for CC# and SSNs, limit unauthorized file transfers and control non-work related web surfing
  - Stream-based, not file-based, for real-time performance
    - *Uniform signature engine scans for all content/threats in single pass*
    - *Low latency, high throughput hardware accelerated engine*
  - Scan for sensitive data (CC# & SSN) and control file type transmissions
  - Protect against a wide range of threats, including viruses, spyware, and vulnerability exploits (IPS)
  - Web filtering enabled via fully integrated URL database
    - *Local database ensure highly scalable solution (1,000’s URLs/sec)*

Single-Pass Parallel Processing™ (SP3) Architecture



Single Pass

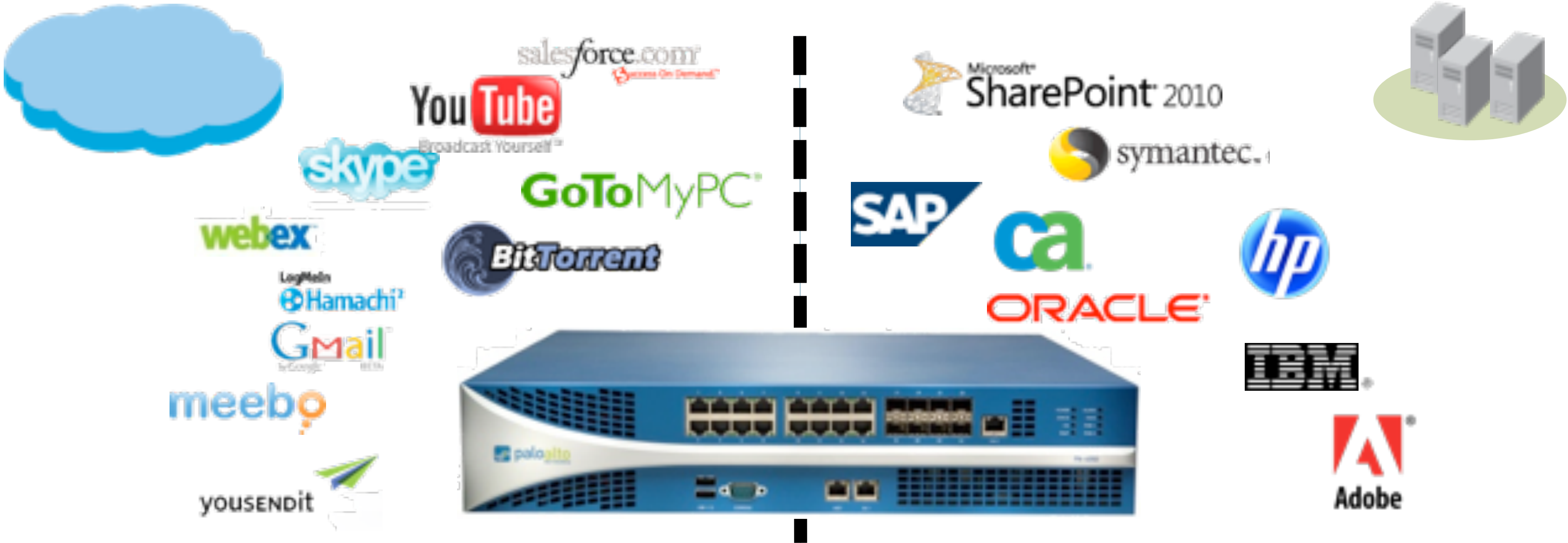
- Operations once per packet
  - Traffic classification (app identification)
  - User/group mapping
  - Content scanning – threats, URLs, confidential data
- One policy

Parallel Processing

- Function-specific parallel processing hardware engines
- Separate data/control planes

Up to 10Gbps, Low Latency

Transforming The Perimeter and Datacenter



- Application visibility and control
- Threat prevention for allowed application traffic
- Unified policy

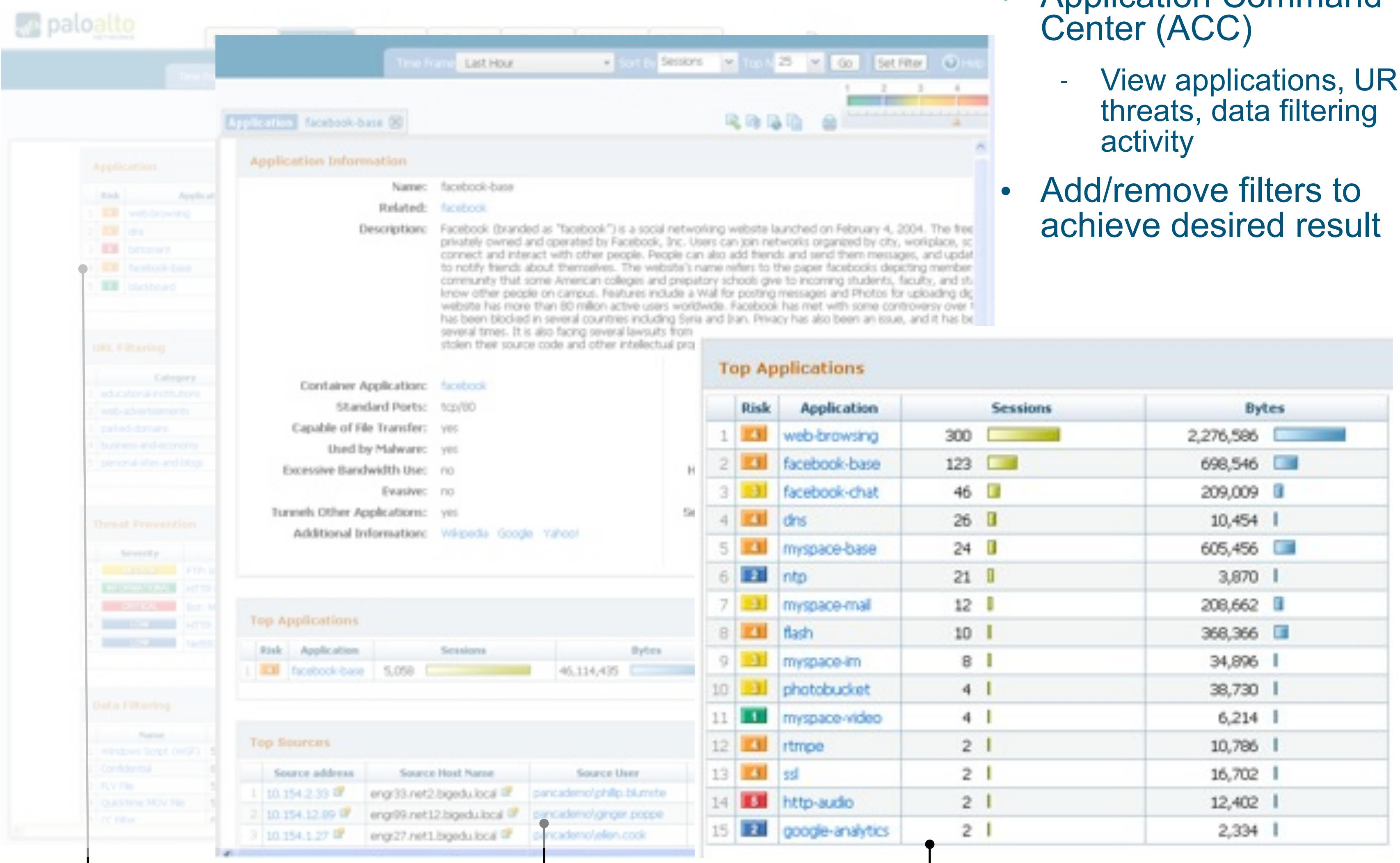
- High-performance firewalling and threat prevention
- Application and user-based segmentation
- Identification and control of rogue applications

Perimeter

Datacenter

Comprehensive View of Applications, Users & Content

- Application Command Center (ACC)
  - View applications, URLs, threats, data filtering activity
- Add/remove filters to achieve desired result



Application Information

Name: facebook-base
Related: facebook
Description: Facebook (branded as "facebook") is a social networking website launched on February 4, 2004. The free privately owned and operated by Facebook, Inc. Users can join networks organized by city, workplace, sc connect and interact with other people. People can also add friends and send them messages, and updat to notify friends about themselves. The website's name refers to the paper facebooks depicting member community that some American colleges and prepatory schools give to incoming students, faculty, and st know other people on campus. Features include a Wall for posting messages and Photos for uploading dig website has more than 80 million active users worldwide. Facebook has met with some controversy over t has been blocked in several countries including Syria and Iran. Privacy has also been an issue, and it has be several times. It is also facing several lawsuits from stolen their source code and other intellectual pro

Container Application: facebook
Standard Ports: tcp/80
Capable of File Transfer: yes
Used by Malware: yes
Excessive Bandwidth Use: no
Evasive: no
Tunnels Other Applications: yes
Additional Information: Wikipedia Google Yahoo!

Top Applications

	Risk	Application	Sessions	Bytes
1	4	facebook-base	5,058	46,114,435

Top Sources

	Source address	Source Host Name	Source User
1	10.154.2.33	engr33.net2.bigedu.local	pancademo\phillip.blumte
2	10.154.12.99	engr99.net12.bigedu.local	pancademo\ginger.poppe
3	10.154.1.27	engr27.net1.bigedu.local	pancademo\ellen.cook

Top Applications

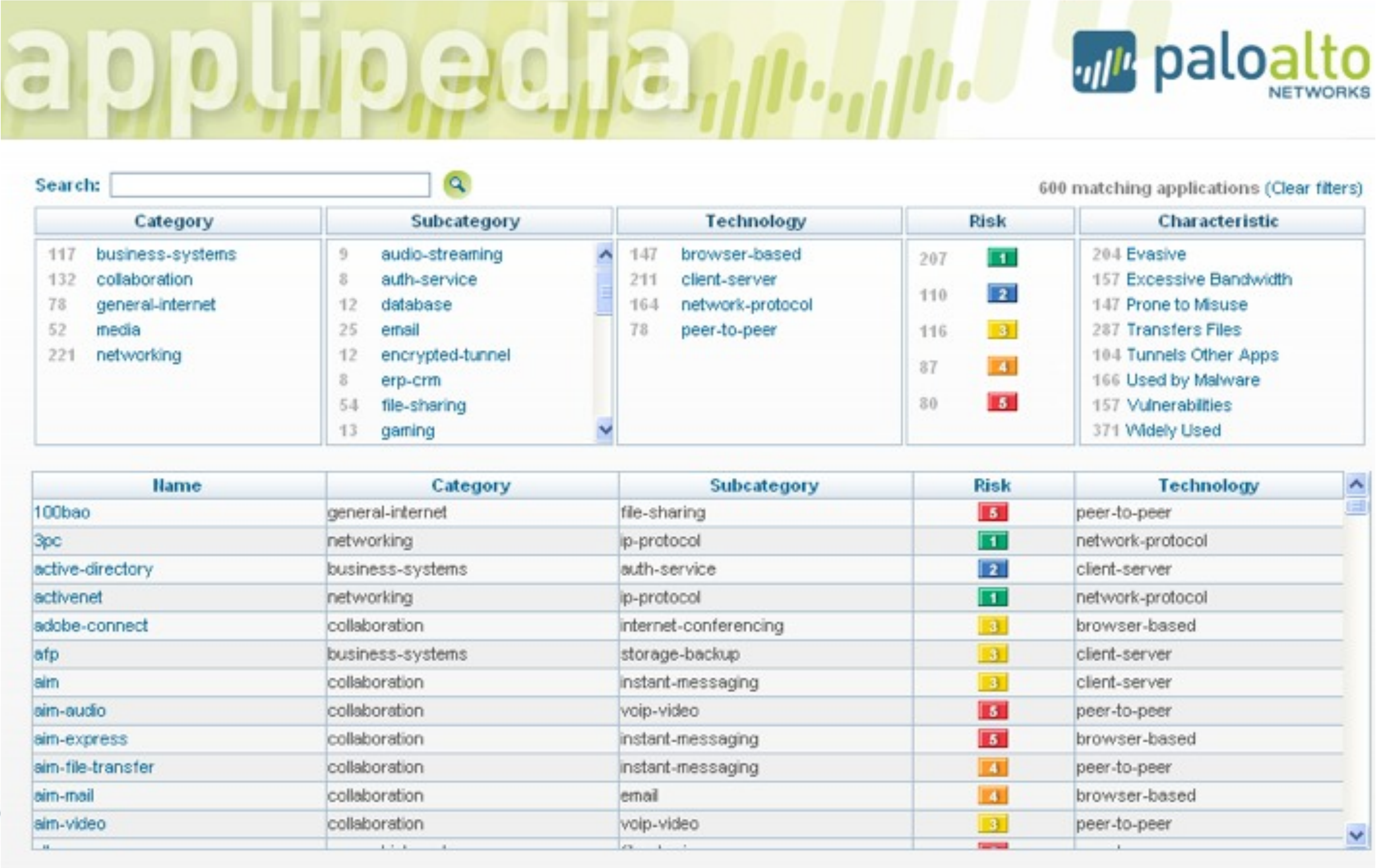
	Risk	Application	Sessions	Bytes
1	4	web-browsing	300	2,276,586
2	4	facebook-base	123	698,546
3	3	facebook-chat	46	209,009
4	4	dns	26	10,454
5	4	myspace-base	24	605,456
6	2	ntp	21	3,870
7	3	myspace-mail	12	208,662
8	4	flash	10	368,366
9	3	myspace-im	8	34,896
10	3	photobucket	4	38,730
11	1	myspace-video	4	6,214
12	4	rtmpe	2	10,786
13	4	ssl	2	16,702
14	5	http-audio	2	12,402
15	2	google-analytics	2	2,334

Filter on Facebook-base

Filter on Facebook-base and user cook

Remove Facebook to expand view of cook

Unmatched Application Expertise



Search:

600 matching applications (Clear filters)

Category	
117	business-systems
132	collaboration
78	general-internet
52	media
221	networking

Subcategory	
9	audio-streaming
8	auth-service
12	database
25	email
12	encrypted-tunnel
8	erp-crm
54	file-sharing
13	gaming

Technology	
147	browser-based
211	client-server
164	network-protocol
78	peer-to-peer

Risk	
207	1
110	2
116	3
87	4
80	5

Characteristic	
204	Evasive
157	Excessive Bandwidth
147	Prone to Misuse
287	Transfers Files
104	Tunnels Other Apps
166	Used by Malware
157	Vulnerabilities
371	Widely Used

Name	Category	Subcategory	Risk	Technology
100bao	general-internet	file-sharing	5	peer-to-peer
3pc	networking	ip-protocol	1	network-protocol
active-directory	business-systems	auth-service	2	client-server
activenet	networking	ip-protocol	1	network-protocol
adobe-connect	collaboration	internet-conferencing	3	browser-based
afp	business-systems	storage-backup	3	client-server
aim	collaboration	instant-messaging	3	client-server
aim-audio	collaboration	voip-video	5	peer-to-peer
aim-express	collaboration	instant-messaging	5	browser-based
aim-file-transfer	collaboration	instant-messaging	4	peer-to-peer
aim-mail	collaboration	email	4	browser-based
aim-video	collaboration	voip-video	3	peer-to-peer

PAN-OS Core Firewall Features

Visibility and control of applications, users and content complement core firewall features

- Strong networking foundation
  - Dynamic routing (BGP, OSPF, RIPv2)
  - Tap mode – connect to SPAN port
  - Virtual wire (“Layer 1”) for true transparent in-line deployment
  - L2/L3 switching foundation
  - Policy-based forwarding
- VPN
  - Site-to-site IPSec VPN
  - SSL VPN
- QoS traffic shaping
  - Max/guaranteed and priority
  - By user, app, interface, zone, & more
  - Real-time bandwidth monitor
- Zone-based architecture
  - All interfaces assigned to security zones for policy enforcement
- High Availability
  - Active / passive
  - Configuration and session synchronization
  - Path, link, and HA monitoring
- Virtual Systems
  - Establish multiple virtual firewalls in a single device (PA-4000 and PA-2000 Series only)
- Simple, flexible management
  - CLI, Web, Panorama, SNMP, Syslog

PA-4060

PA-4050

PA-4020

PA-2050

PA-2020

PA-500

Next-Generation Firewalls Are Network Security

PLEXUS

THE GREAT ATLANTIC & PACIFIC TEA CO.

BNP PARIBAS

Virgin media

Tyson

Reliance Steel & Aluminum Co.

IDT

DELTA
see what Delta can do

DTE Energy

T · · ·

Western & Southern Life
A member of Western & Southern Financial Group

Elavon

ebaY

KDDI

GE

QUALCOMM

CNP

ACUITY

FannieMae

tellabs

eDF Trading

PEUGEOT

BON·TON
COME TO THE RIGHT PLACE

Genentech
IN BUSINESS FOR LIFE

CYTEC

Westpac

SONY

Bloomberg

Western Refining

ConocoPhillips

MERCURY
INSURANCE GROUP

Investec

Genworth Financial

SanDisk

ARAMARK

TOYOTA

TOSHIBA

Weatherford

WERNER ENTERPRISES

ADP Automatic Data Processing, Inc.

hp

THALES

Kimberly-Clark

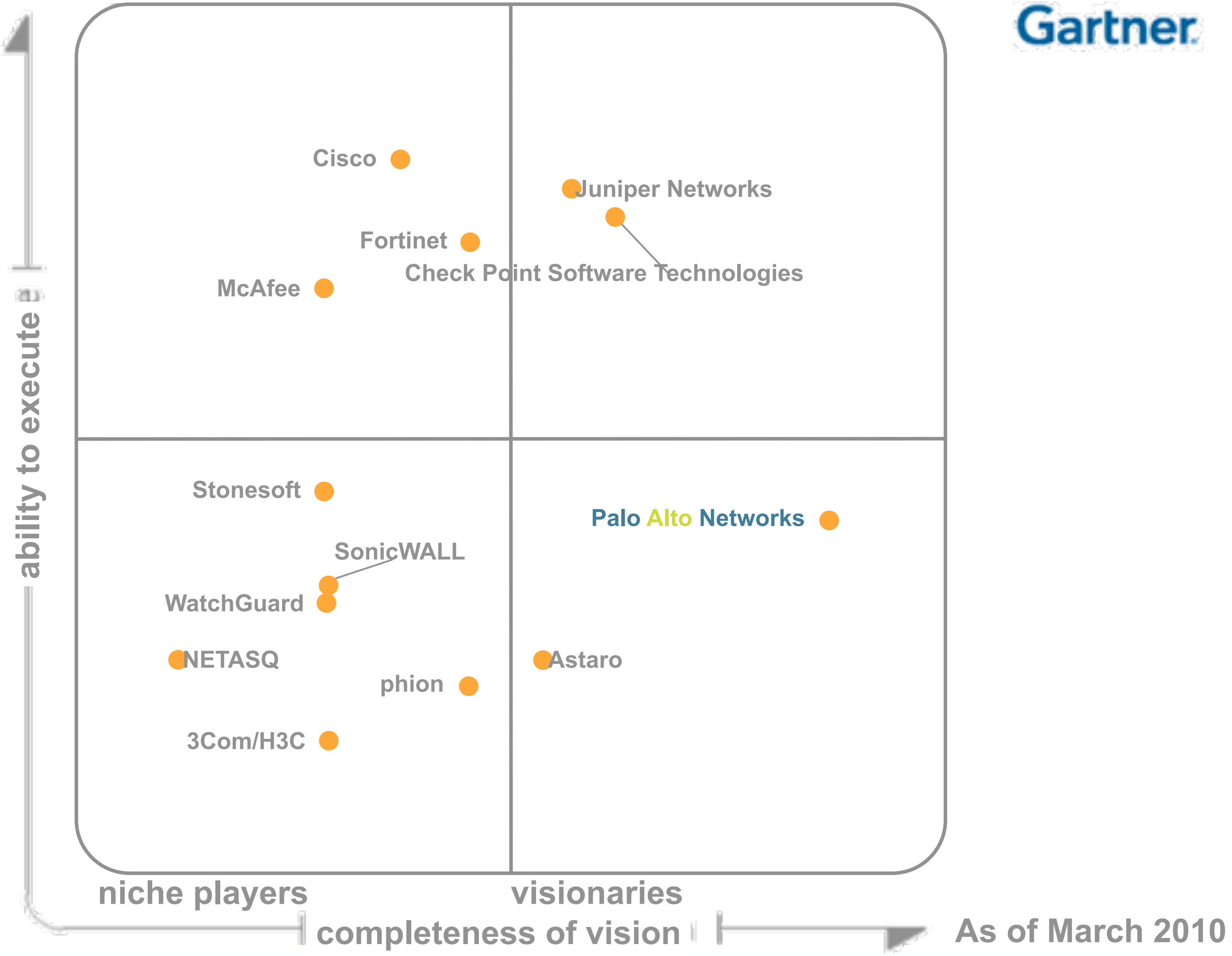
中国银行
BANK OF CHINA

PINNACLE WEST
CAPITAL CORPORATION

UNIVISION

paloalto
NETWORKS

2010 Magic Quadrant for Enterprise Network Firewalls



As of March 2010

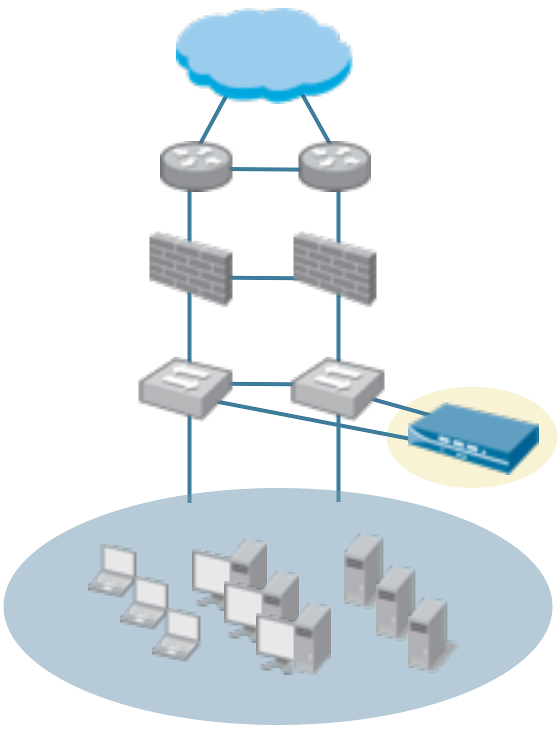
Source: Gartner

Addresses Three Key Business Problems

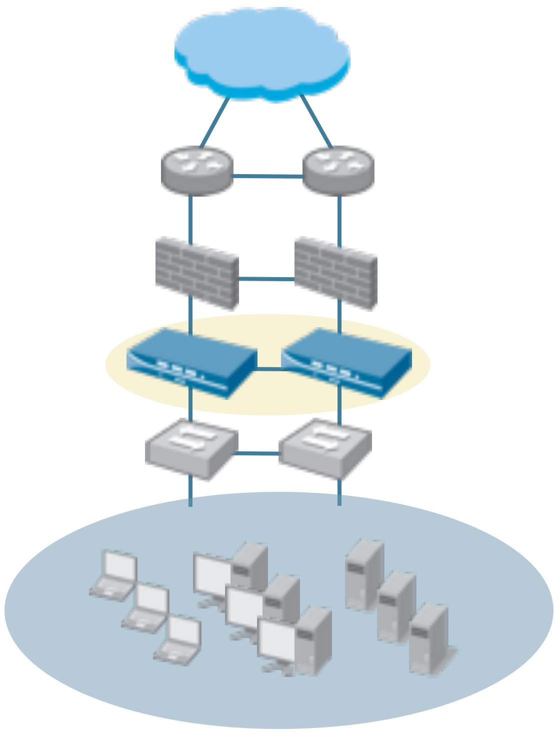
- **Identify and Control Applications**
  - Visibility of 1000+ applications, regardless of port, protocol, encryption, or evasive tactic
  - Fine-grained control over applications (allow, deny, limit, scan, shape)
  - Addresses the key deficiencies of legacy firewall infrastructure
- **Prevent Threats**
  - Stop a variety of threats – exploits (by vulnerability), viruses, spyware
  - Stop leaks of confidential data (e.g., credit card #, social security #)
  - Stream-based engine ensures high performance
  - Enforce acceptable use policies on users for general web site browsing
- **Simplify Security Infrastructure**
  - Put the firewall at the center of the network security infrastructure
  - Reduce complexity in architecture and operations

Flexible Deployment Options

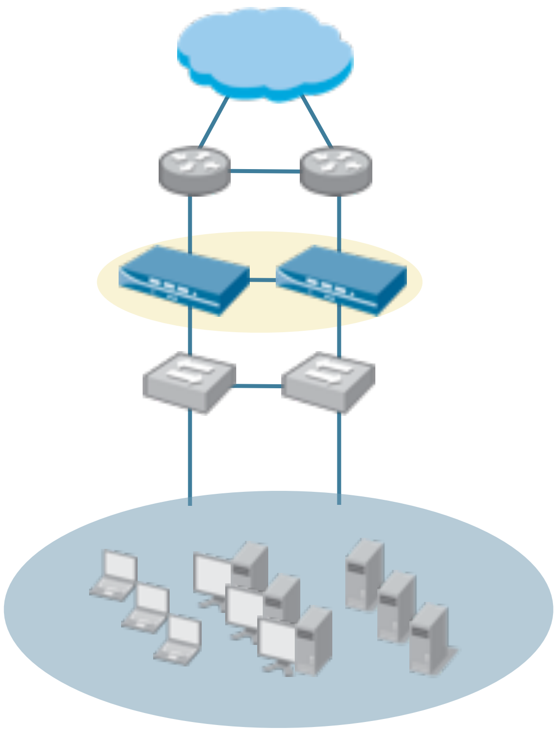
Visibility



Transparent In-Line



Firewall Replacement

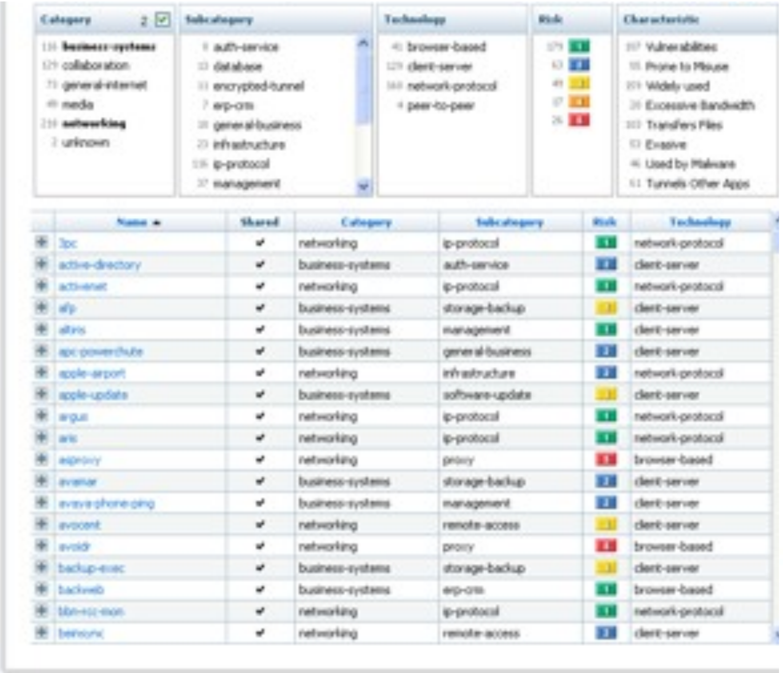


- Application, user and content visibility without inline deployment

- IPS with app visibility & control
- Consolidation of IPS & URL filtering

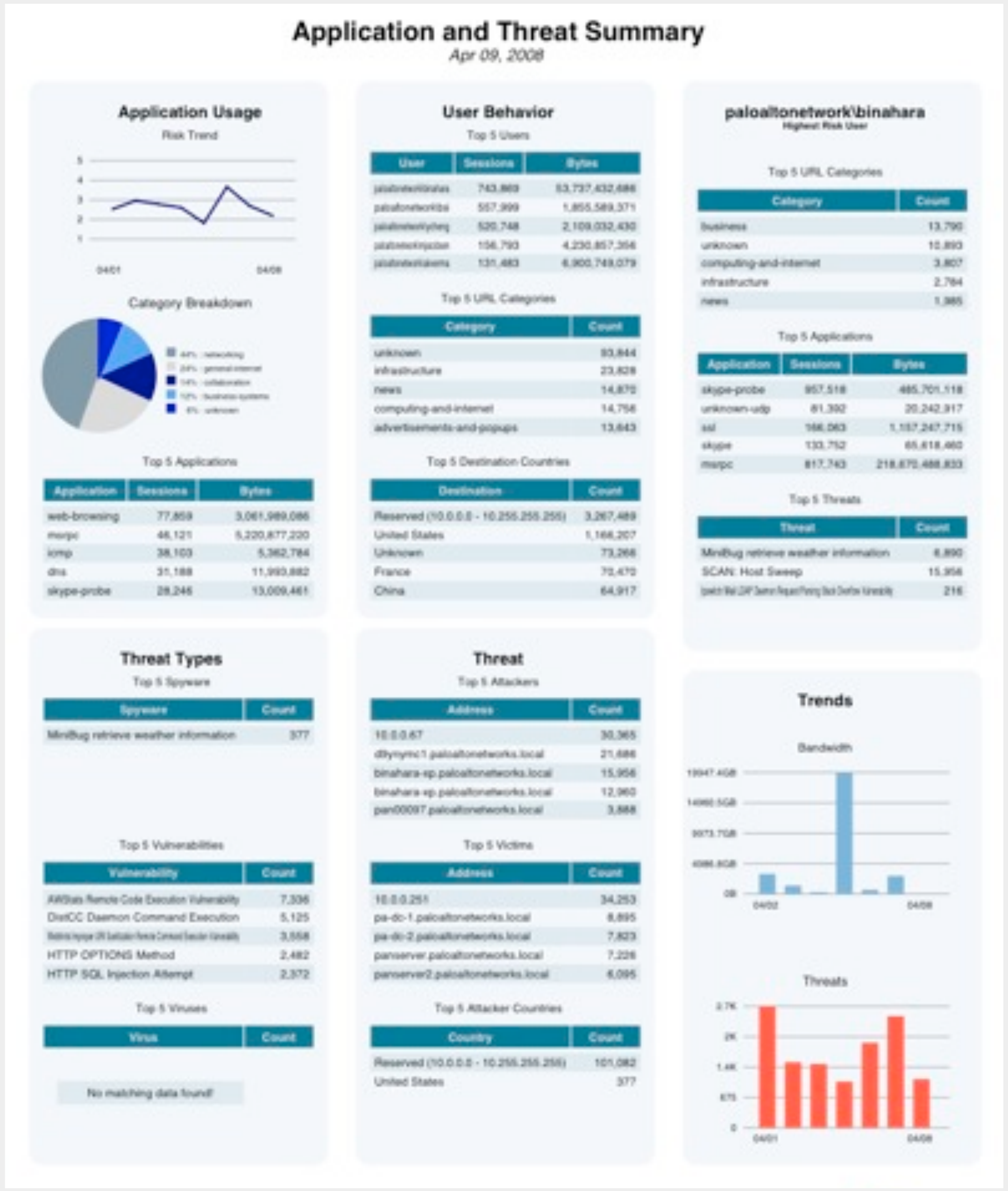
- Firewall replacement with app visibility & control
- Firewall + IPS
- Firewall + IPS + URL filtering

Enables Visibility Into Applications, Users, and Content



Category 2 ☑	Subcategory	Technology	Risk	Characteristic
118 **business-systems**	8 auth-service	41 browser-based	179 1	107 Vulnerabilities
129 collaboration	13 database	129 client-server	63 2	55 Prone to Misuse
71 general-internet	11 encrypted-tunnel	168 network-protocol	49 3	203 Widely used
49 media	7 erp-crm	4 peer-to-peer	37 4	28 Excessive Bandwidth
218 **networking**	18 general-business		26 5	103 Transfers Files
2 unknown	23 infrastructure			53 Evasive
	116 ip-protocol			46 Used by Malware
	37 management			61 Tunnels Other Apps

	Name ▲	Shared	Category	Subcategory	Risk	Technology
⊞	3pc	✓	networking	ip-protocol	1	network-protocol
⊞	active-directory	✓	business-systems	auth-service	2	client-server
⊞	activenet	✓	networking	ip-protocol	1	network-protocol
⊞	afp	✓	business-systems	storage-backup	3	client-server
⊞	altiris	✓	business-systems	management	1	client-server
⊞	apc-powerchute	✓	business-systems	general-business	2	client-server
⊞	apple-airport	✓	networking	infrastructure	2	network-protocol
⊞	apple-update	✓	business-systems	software-update	3	client-server
⊞	argus	✓	networking	ip-protocol	1	network-protocol
⊞	aris	✓	networking	ip-protocol	1	network-protocol
⊞	asproxy	✓	networking	proxy	5	browser-based
⊞	avamar	✓	business-systems	storage-backup	2	client-server
⊞	avaya-phone-ping	✓	business-systems	management	2	client-server
⊞	avocent	✓	networking	remote-access	3	client-server
⊞	avoidr	✓	networking	proxy	5	browser-based
⊞	backup-exec	✓	business-systems	storage-backup	3	client-server
⊞	backweb	✓	business-systems	erp-crm	1	browser-based
⊞	bbn-rcc-mon	✓	networking	ip-protocol	1	network-protocol
⊞	beinsync	✓	networking	remote-access	2	client-server



Application and Threat Summary

Apr 09, 2008

Application Usage

Top 5 Applications

Application	Sessions	Bytes
web-browsing	77,859	3,061,989,086
msrpc	46,121	5,220,877,220
icmp	38,103	5,362,784
dns	31,188	11,993,882
skype-probe	28,246	13,009,461

User Behavior

Top 5 Users

User	Sessions	Bytes
paloaltonetwork\binahara	743,869	53,737,432,686
paloaltonetwork\bsi	557,999	1,855,589,371
paloaltonetwork\ycheq	520,748	2,109,032,430
paloaltonetwork\jscian	156,793	4,230,857,356
paloaltonetwork\akers	131,483	6,900,749,079

Top 5 URL Categories

Category	Count
unknown	93,844
infrastructure	23,828
news	14,870
computing-and-internet	14,756
advertisements-and-popups	13,643

Top 5 Destination Countries

Destination	Count
Reserved (10.0.0.0 - 10.255.255.255)	3,267,489
United States	1,166,207
Unknown	73,268
France	70,470
China	64,917

paloaltonetwork\binahara

Highest Risk User

Top 5 URL Categories

Category	Count
business	13,790
unknown	10,893
computing-and-internet	3,807
infrastructure	2,764
news	1,385

Top 5 Applications

Application	Sessions	Bytes
skype-probe	957,518	485,701,118
unknown-udp	81,392	20,242,917
ssl	166,063	1,157,247,715
skype	133,752	65,618,460
msrpc	817,743	218,670,488,833

Top 5 Threats

Threat	Count
MiniBug retrieve weather information	6,890
SCAN: Host Sweep	15,958
Ipswitch IMail LDAP Daemon Request Parsing Stack Overflow Vulnerability	216

Threat Types

Top 5 Spyware

Spyware	Count
MiniBug retrieve weather information	377

Top 5 Vulnerabilities

Vulnerability	Count
AWStats Remote Code Execution Vulnerability	7,306
DistCC Daemon Command Execution	5,125
[illegible] Remote Command Execution Vulnerability	3,558
HTTP OPTIONS Method	2,482
HTTP SQL Injection Attempt	2,372

Top 5 Viruses

Virus	Count
No matching data found!	

Threat

Top 5 Attackers

Address	Count
10.0.0.67	30,365
dllynymc1.paloaltonetworks.local	21,686
binahara-xp.paloaltonetworks.local	15,956
binahara-xp.paloaltonetworks.local	12,960
pan00097.paloaltonetworks.local	3,888

Top 5 Victims

Address	Count
10.0.0.251	34,253
pa-dc-1.paloaltonetworks.local	8,895
pa-dc-2.paloaltonetworks.local	7,823
panserver.paloaltonetworks.local	7,226
panserver2.paloaltonetworks.local	6,095

Top 5 Attacker Countries

Country	Count
Reserved (10.0.0.0 - 10.255.255.255)	101,082
United States	377

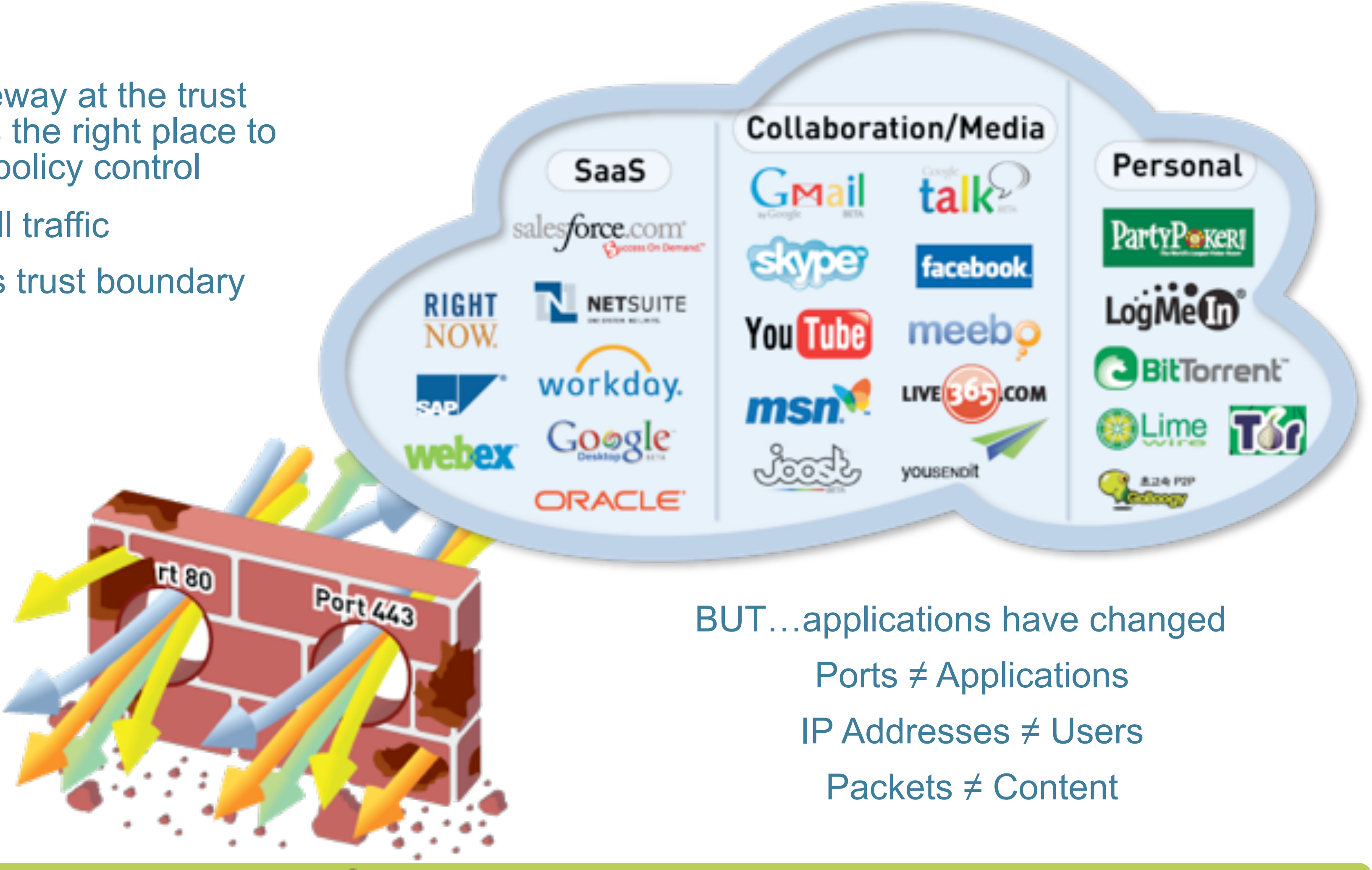
Trends

So What’s Next?

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

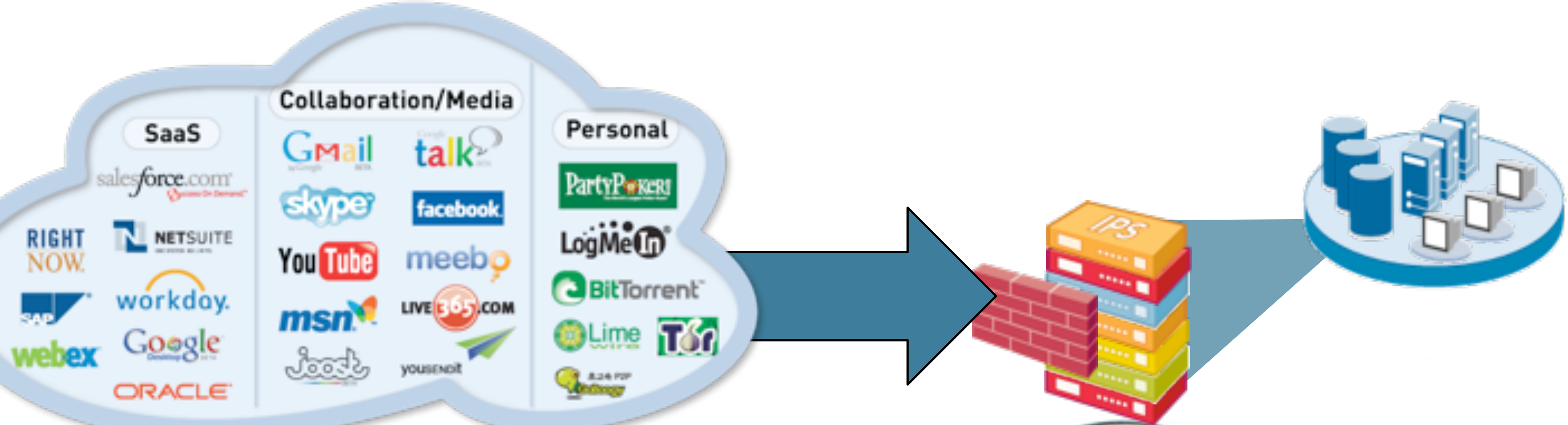
Ports ≠ Applications

IP Addresses ≠ Users

Packets ≠ Content

This was the problem we set out to solve.

But We Didn’t Just Re-Invent the Firewall…



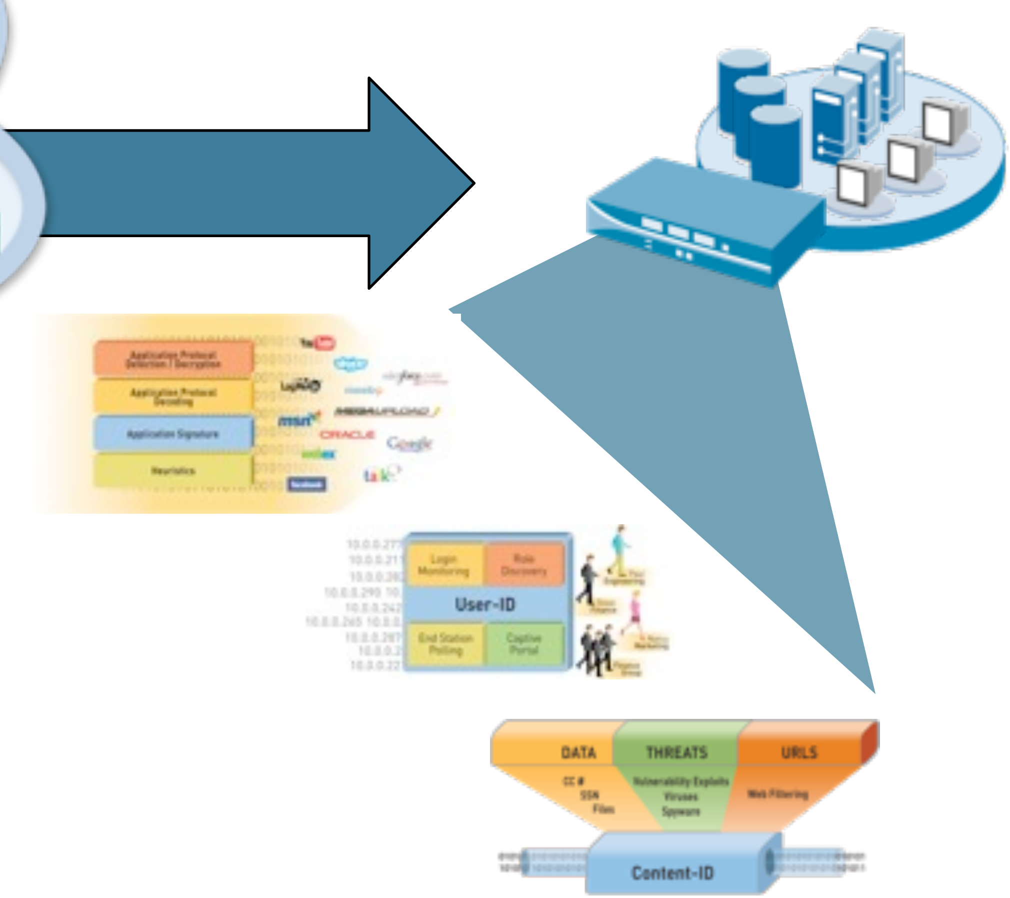
Ports
IP Addresses
Threat Patterns
URLs

The old way…

- Access control: firewall/VPN
- Threat prevention: IPS/AV
- Content control: URL filtering, proxies, DLP

…We Are Re-Inventing Network Security

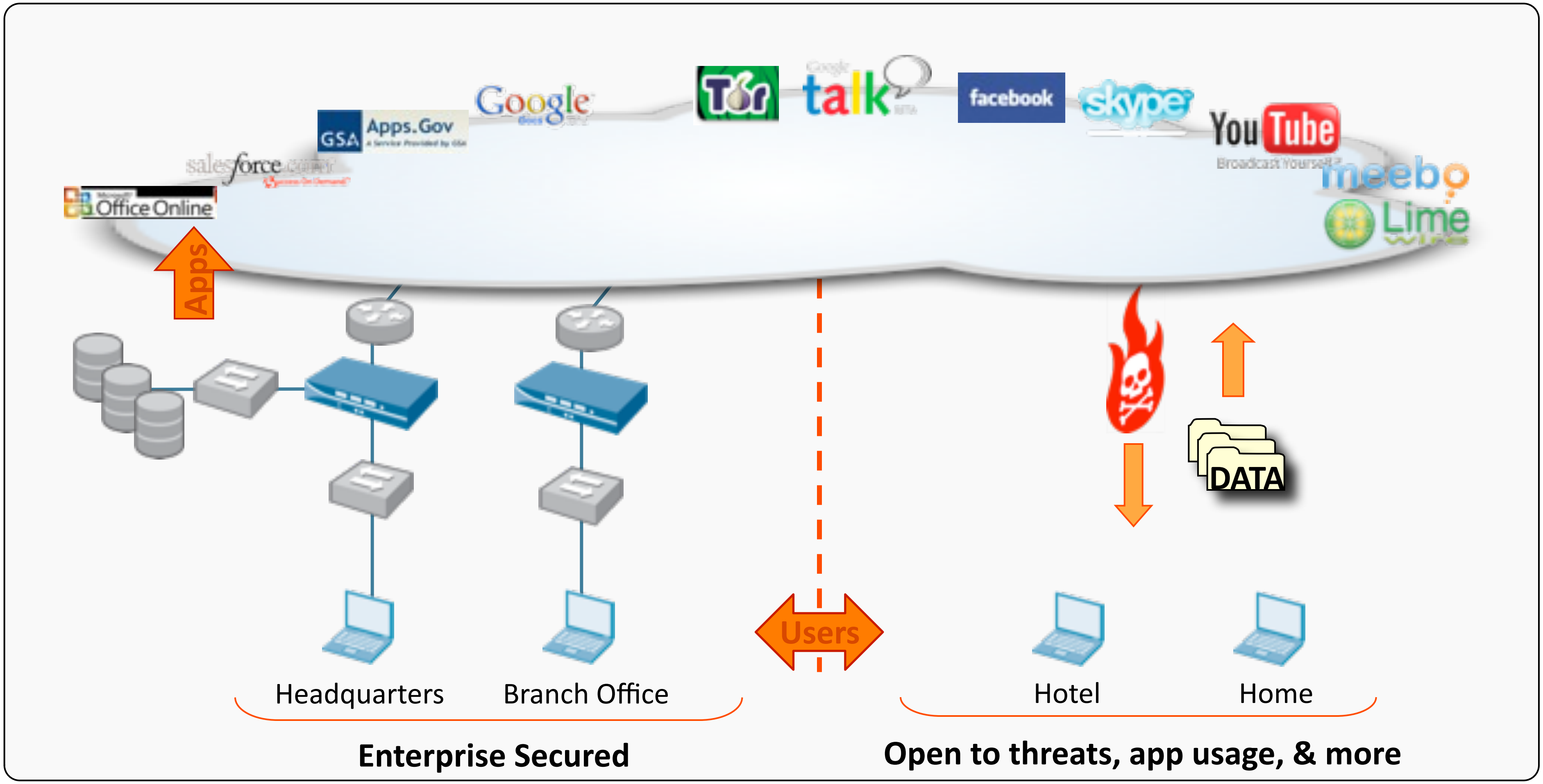
SaaS
Collaboration/Media
Personal



- Next-generation firewalls provide visibility and control of applications, users, and content
- App-ID, User-ID, Content-ID enable organizations to simplify network security
  - Access control
  - Threat prevention
  - Content control

Solved the "Inside" Problem - But Users Leave…

How do you secure your applications and your users when they are both moving off the "controlled" network?

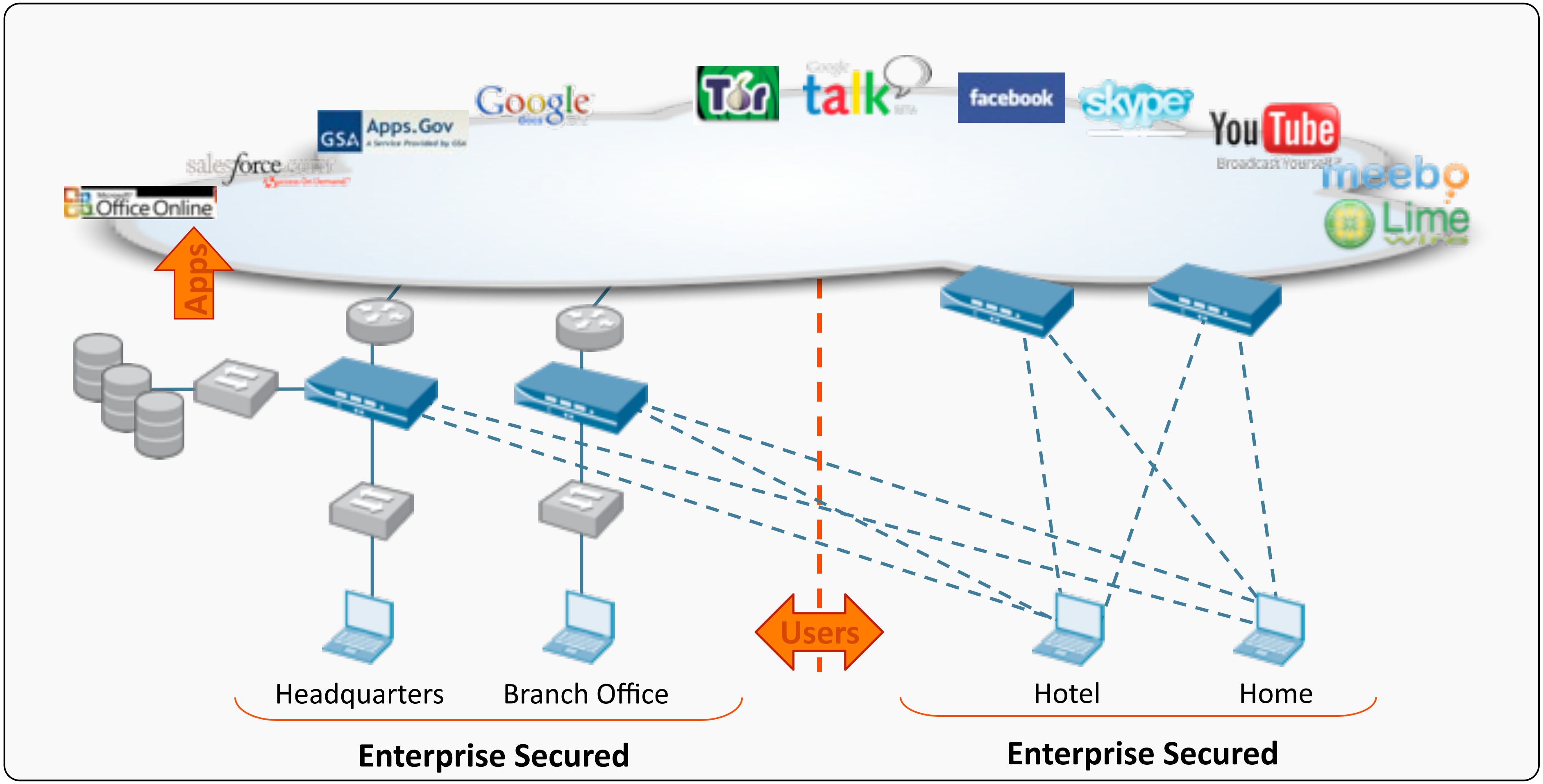


Traditional Approaches Don't Work

- Client software
  - File/process-oriented
  - Overloaded
  - Coarse-grained management
- Proxy/proxy in the cloud
  - Subset of traffic
  - Web-focused
  - Coarse-grained management
- Traditional VPN/port-based approach
  - Sees all traffic
  - Often highly centralized
  - No intelligence in controls

Get the Same Visibility and Control for All Users

Palo Alto Networks GlobalProtect™ will enable organizations to safely enable applications, regardless of user location



Palo Alto Networks Continuing to Innovate

- Enterprises basing network security on Palo Alto Networks next-generation firewalls
- GlobalProtect^{TM} will bring roaming users into next-generation firewall-based control
  - Applications/Users/Content
- GlobalProtect^{TM} will support Windows-based machines initially
  - Windows 7 (32 & 64-bit)
  - Windows Vista (32 & 64-bit)
  - Windows XP
- Pricing: subscription (per firewall, not user-based)
- Available end of 2010

paloalto
NETWORKS

the network security company™