



**Smart Today, Secure Tomorrow:  
Five Essentials for Future-Proof Content Security**



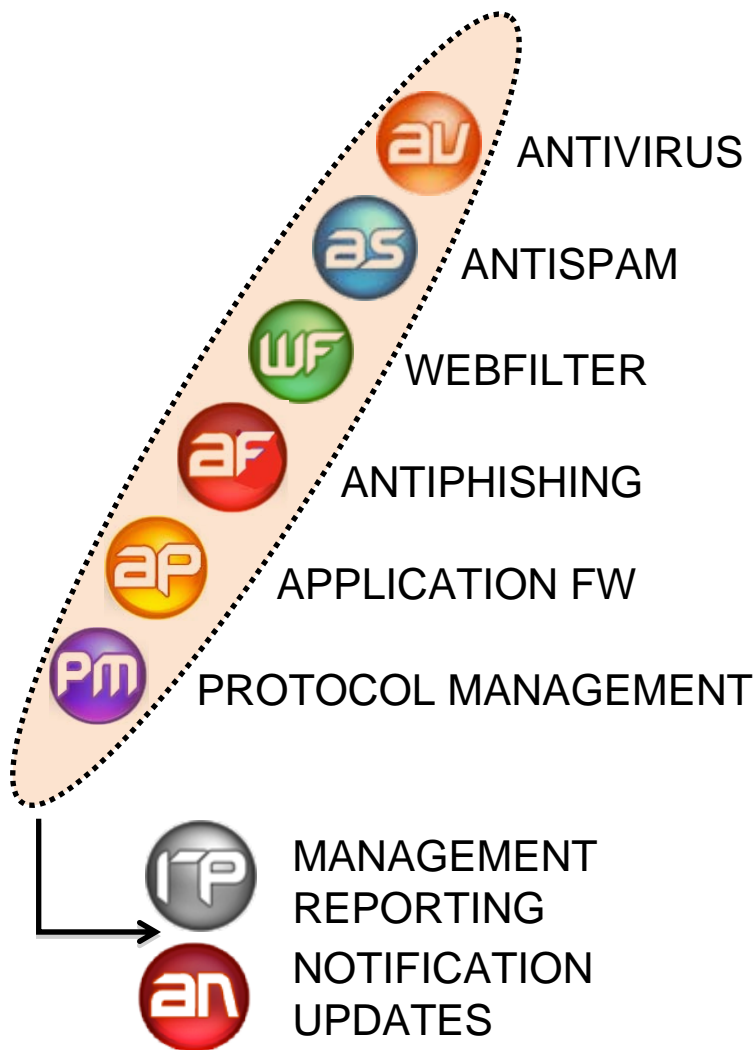
**Joel Silberman**  
**Vice President North America**

# Optenet Background

## Global Security Company

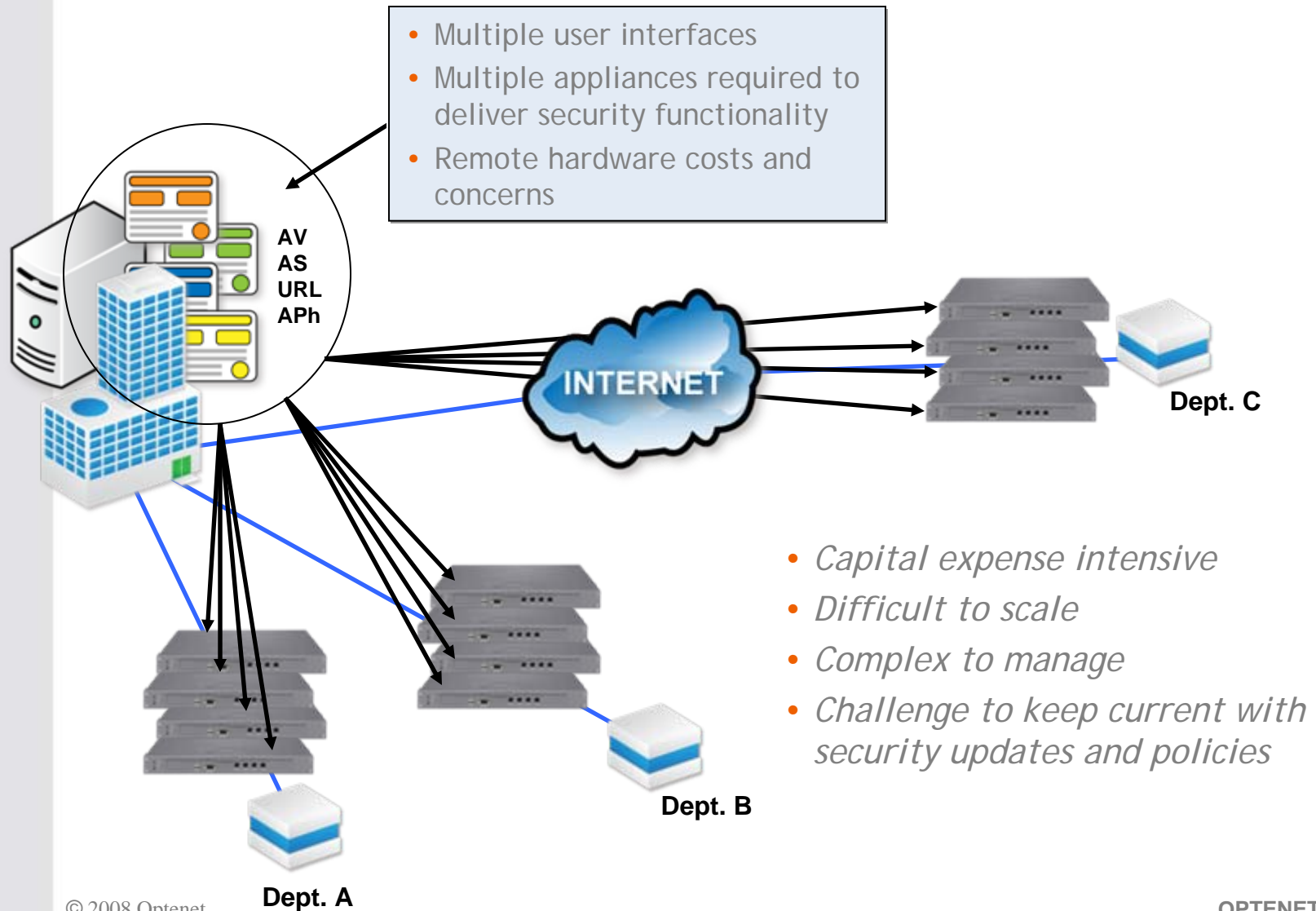
- Founded in 1997
- Headquartered in Madrid, Spain
  - Global presence: USA, EMEA, LATAM, Australia
  - R&D centers in North America, Europe and LATAM
  - Launched North America operations in June 2008
- Leading provider of content security solutions to service providers
  - More than **50 large network operators** worldwide use Optenet solutions: **O2, Orange, and Telefónica**
  - Provides content security for **100 million users**
- Blue chip enterprise customers: **McDonalds, NHS, Daimler AG**

# Optenet Content Security Suite

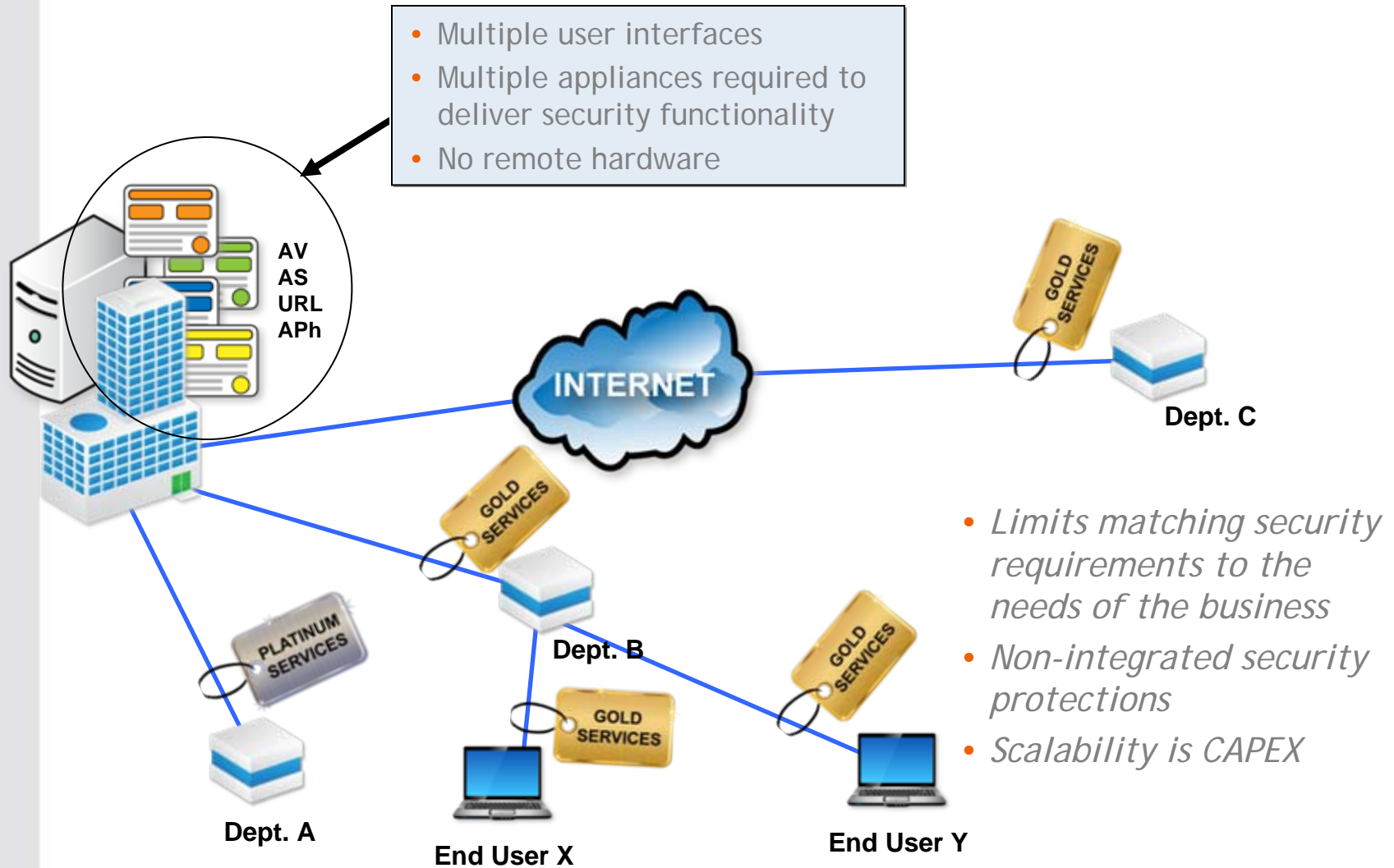


- Protection against every type of Web and eMail threat
- Integrated security suite with centralized management and distributed operation
- Market-leading performance
- Extreme scalability and ease of deployment
- **Multi-tenant architecture enables dramatic improvement in overall TCO across the enterprise, branch offices and remote users**

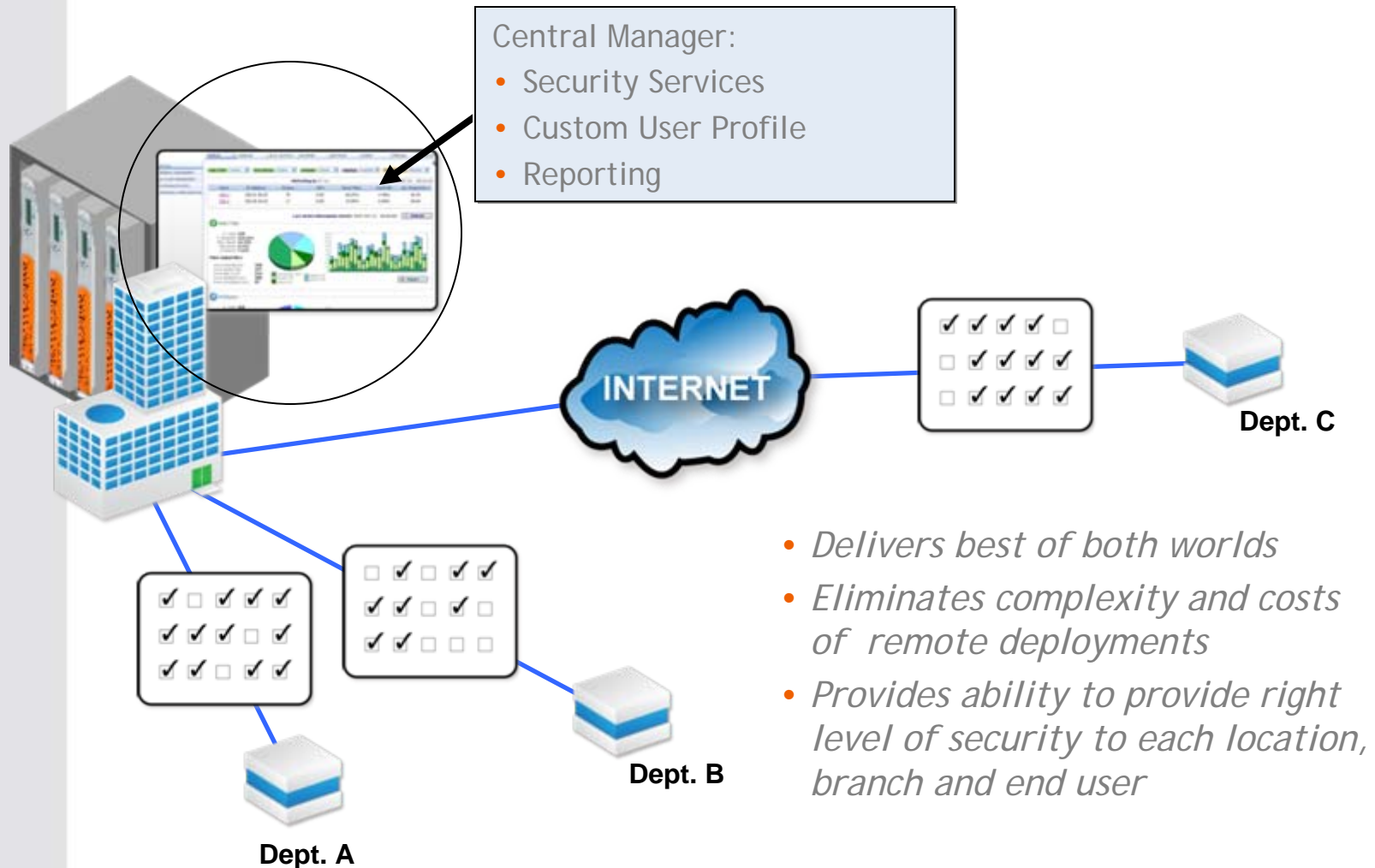
# Traditional Security Deployment: Multiple Appliances in the Enterprise



# Centralized Security Deployment: Limited security protection & flexibility



# Customized Security Services: Multi-Tenancy in the Enterprise



# Summary

Optenet Security Suite provides:

- Complete and integrated content security solution
- TCO benefits across the enterprise
- Scalable, flexible architecture for today and future security needs

# The five content-security essentials for a future-proof strategy

**Chenxi Wang, Ph.D.**  
Principal Analyst  
Forrester Research

December, 2008

# What is content security?

- Email, web, IM, and other communication protocols
  - » Moves content in and out of corporation
- Control and management of content-related policies
  - » Mitigate content-borne threats
  - » Control data leaks
  - » Regulate content applications
  - » Gain visibility into usage, activities, and controls

# Content security's changing role in today's dynamic environment

- Web 2.0 is pervasive
- Mobile computing is everywhere
- Unstructured content permeates enterprises
- URL filtering and AV gateway is no longer enough
- Content control policies are getting more complex

# Five essentials for a future-proof solution

- In-the-cloud community intelligence
- Pervasive reputation
- Data leak prevention
- Mobile filtering
- Integration & consolidation



In the cloud community  
intelligence

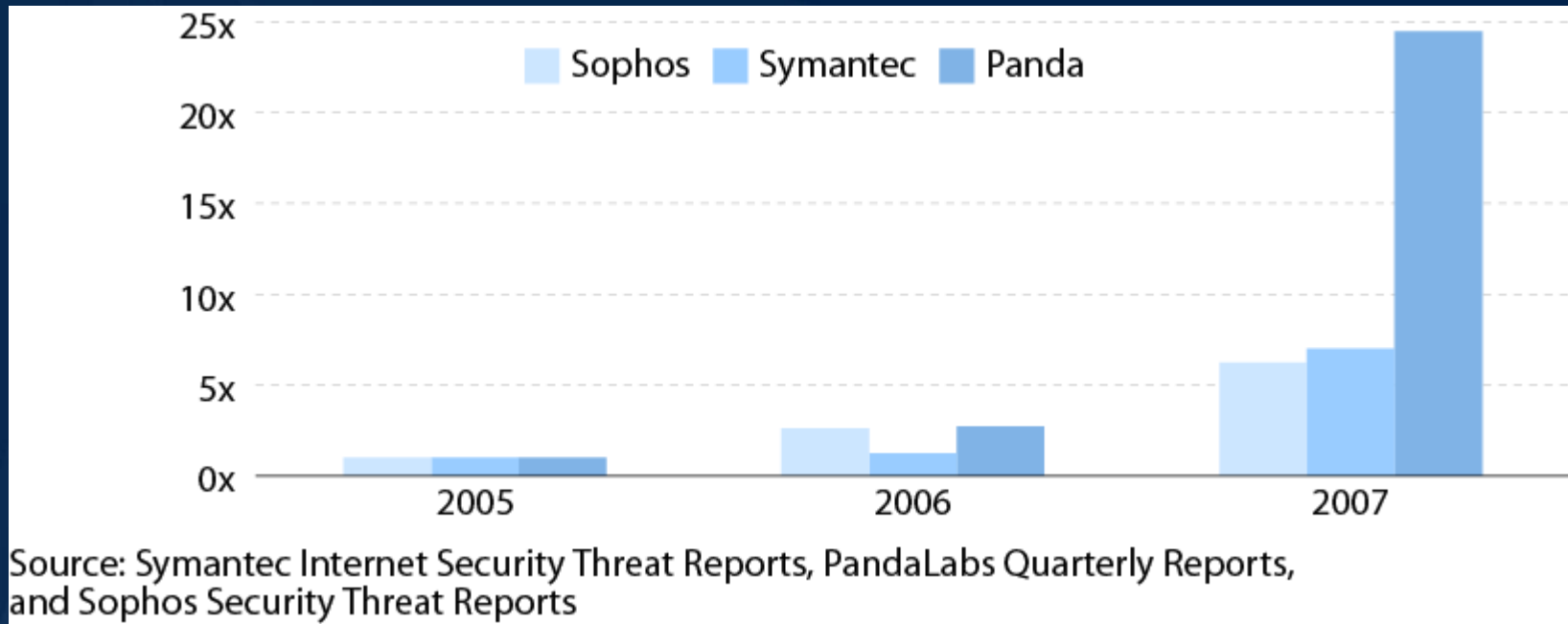
# Utilizing a “big brain” in the cloud



- » Wider visibility into Internet traffic and malicious patterns
- » Obtain more precise threat information quickly
- » Knowledge dissemination benefits everyone

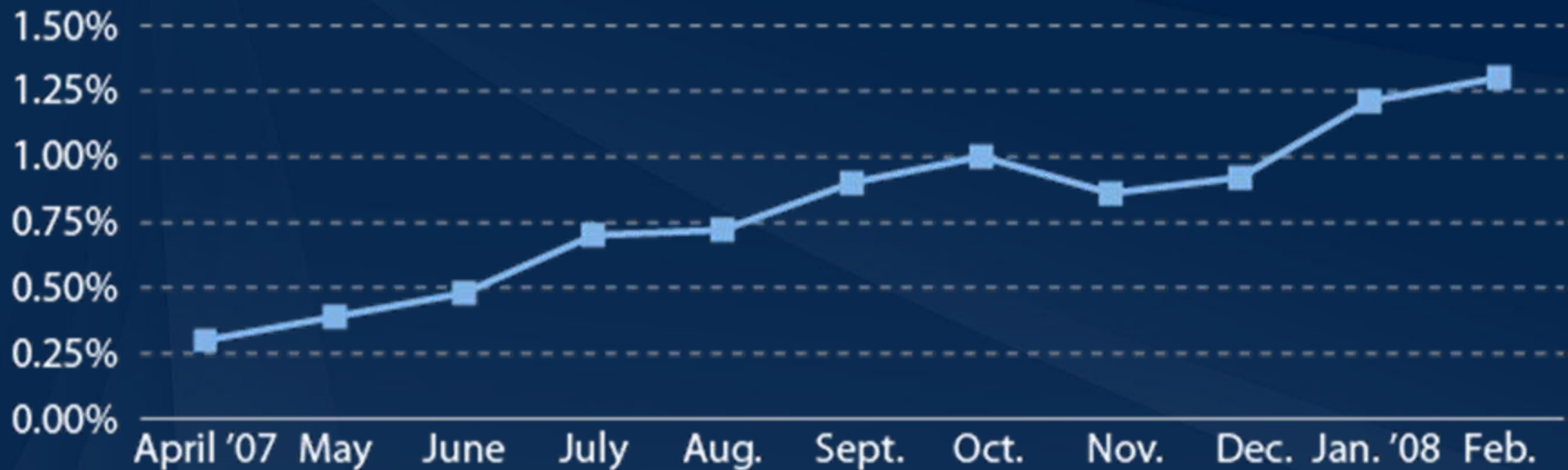
# Malware is reaching epidemic proportions

June 2008 “Threat Report: The Trends And Changing Landscape Of Malware And Internet Threats”



**Soon it'll be infeasible to keep signatures on premise**

# Internet is becoming more dangerous . . .



**Much of that increase is due to legitimate websites gone bad**

Source: "All Your IFRAMEs Point to Us," Google, February 4, 2008

# Community intelligence is a must-have

- In-the-cloud community intelligence is a must for any content security solution
  - » Local knowledge feeds the cloud
- SaaS with the community intelligence as a backdrop
- More things will be moving into the cloud
  - » Management, reporting, even logs
- On-premise presence will become increasingly thin



# Pervasive reputation

# Pervasive reputation

- Today reputation is calculated on IPs, domains, and web sites
- Reputation data will cover files, programs, even online identities
  - » Consider mashups with code reputation
  - » Facebook with application reputation
- Reputation will live in the cloud
- It will be ubiquitous, with a common language



# Data leaks

# Data leaks

- Attacks today are about information assets
- Data leaks over the web is a weak link
  - » WebMail, blogs, wikis, etc.
- What about the other protocols?
  - » WebEx
  - » Instant messaging
  - » Skype
  - » Microsoft OCS
  - » Voice + data + presence

# What are people doing about data leaks?

- Some are doing light-weight data leak protection
- Many are doing nothing
- Content security products' data leak capabilities are not quite mature
- Prediction: content security will work with internal data classification mechanisms



# Mobile filtering

# Road warriors are common place

- Many companies have a mobile workforce
  - » Common to have at least 25% mobile workers
- Simple on-premise approach does not work
- Options
  - » VPN the traffic back in
  - » Enforced proxy
  - » Completely client based

# Mobile workforce is a loophole in corporate policies

- Visibility to corporate directories is important
- Performance is critical
- Seamless experience is the key
- Central management must be supported



# Integration & consolidation

# Integration and consolidation

- Traditionally silo-ed approach
  - » Email, web are treated separately
- Requirements for integration emerge
  - » DLP, management, reporting
- The cloud-intelligence will drive consolidation
- Going forward, other form of communications will also converge

# Five essentials for a future-proof solution

- In-the-cloud community intelligence
- Pervasive reputation
- Data leak prevention
- Mobile filtering
- Integration & consolidation

# Summary

- Look to vendors who have a strong position in these five aspects
  - » Runs a solid in-the-cloud platform
  - » Conducts its own proactive threat research
  - » Understands how to work with content classifiers
  - » Has a strong integration/consolidation strategy
  - » Offers enterprise-grade, centralized management

A person is climbing a dark rock face on the left side of the image. The climber is wearing a dark jacket, pants, and a red backpack. The background shows a vast mountain range with snow-capped peaks under a clear blue sky. The overall scene is dramatic and adventurous.

# Thank you.

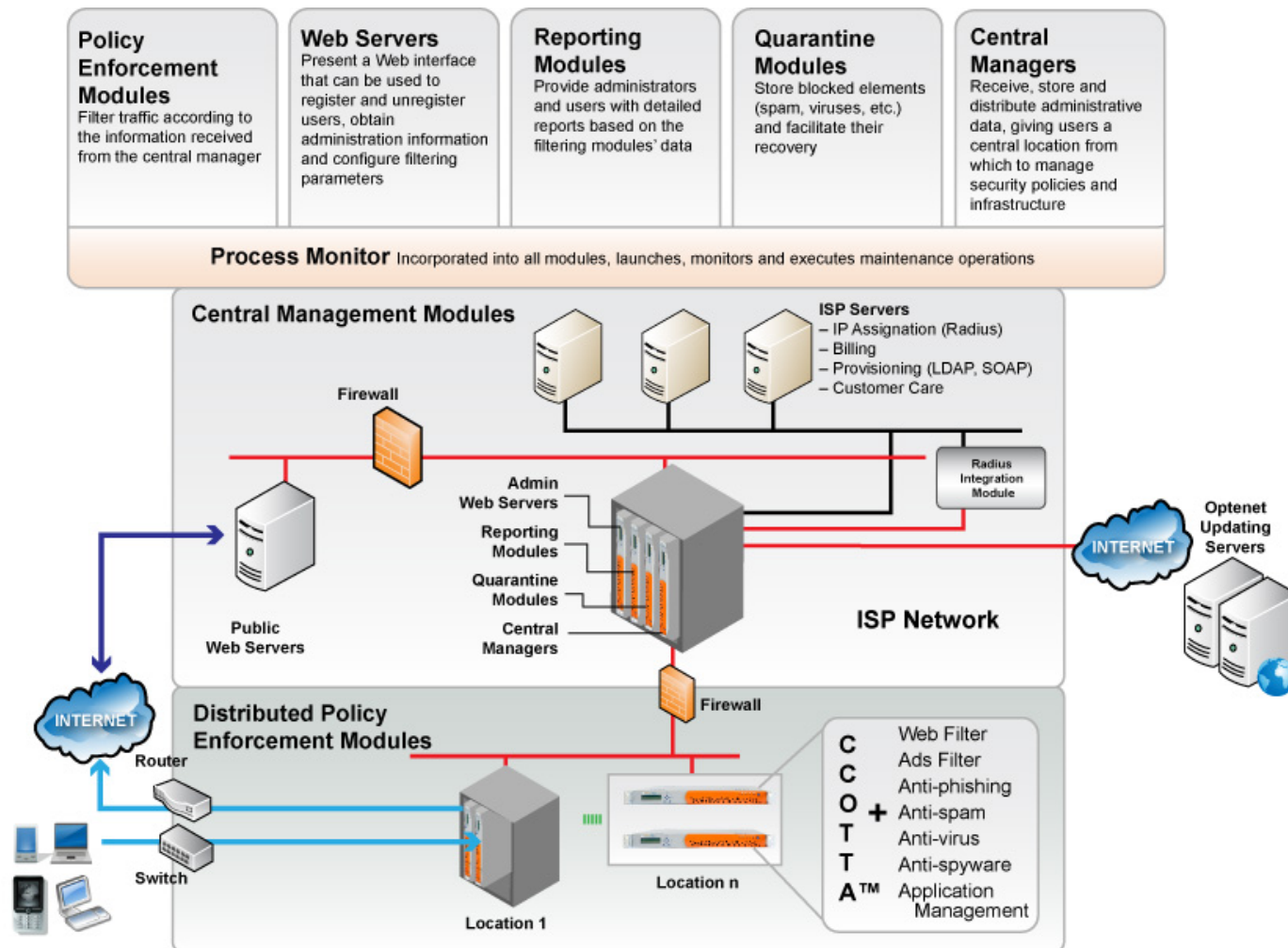
- **Chenxi Wang**  
Principal Analyst  
Forrester Research

- **Email**  
[cwang@forrester.com](mailto:cwang@forrester.com)
- **Blog**  
[blogs.forrester.com/srm](https://blogs.forrester.com/srm)



**Omar Aguirre**  
**Chief Operating Officer, Optenet**

# Distributed Architecture



# Integrated Administration Console

- Real-time central reports Web and mail
- Profiles (per group, equipment or person) and management with common policies
- End point protection centralized network management (remote employees)



The screenshot shows the Optenet Integrated Administration Console interface. At the top, there are seven navigation tabs: GENERAL, WEB/WAP, AUTO. NOTICES, ANTISPAM, ANTIVIRUS, ID5/IPS, FIREWALL, and REPORTER. Below these tabs is a breadcrumb trail: » General » Filtering Policies » Policies. The main content area is titled "Policies" and contains a table with the following columns: Enabled, Service, Policy, Target Group, Profile, Action, and Schedule. A "+ priority" link is visible to the right of the table.

Enabled	Service	Policy	Target Group	Profile	Action	Schedule
On	 Home	News	Optenet Madrid	Categ., Files	Block	Always

# Centralized Management and Reporting

## Security Policies

GENERAL WEB/WAP AUTO. NOTICES ANTISPAM ANTIVIRUS ID5/IPS FIREWALL REPORTER

>> General >> Filtering Policies >> Policies

**Policies**

Enabled	Service	Policy	Target Group	Profile	Action	Schedule	
On	Home	News	Optenet Madrid	Categ., Files	Block	Always	+ priority
On	Enterprise	Deny Skype	All	Services	Block	Always	↑
On	Home	Block multimedia	Optenet Madrid	Connection	Delete	Lunch	
On	Enterprise	Delete Files	All	Web, Files	Delete	Always	Edit
On	Enterprise	Ads	Optenet Madrid	Default	Redirect	Always	Delete
On	Home	Allow mail	All	Connection	Allow	Morning	
On	Enterprise	Block Connections	All	Services	Block	Always	↓
On	Enterprise	Monitor News	All	Categ., Files, Includ. Monitor		Always	
On	Home	Filter	All	Default	Block	Always	- priority

**Customizable** according to parameters:

- **who** (Target group)
- **how** (Profile)
- **what** (Action)
- **when** (Schedule)

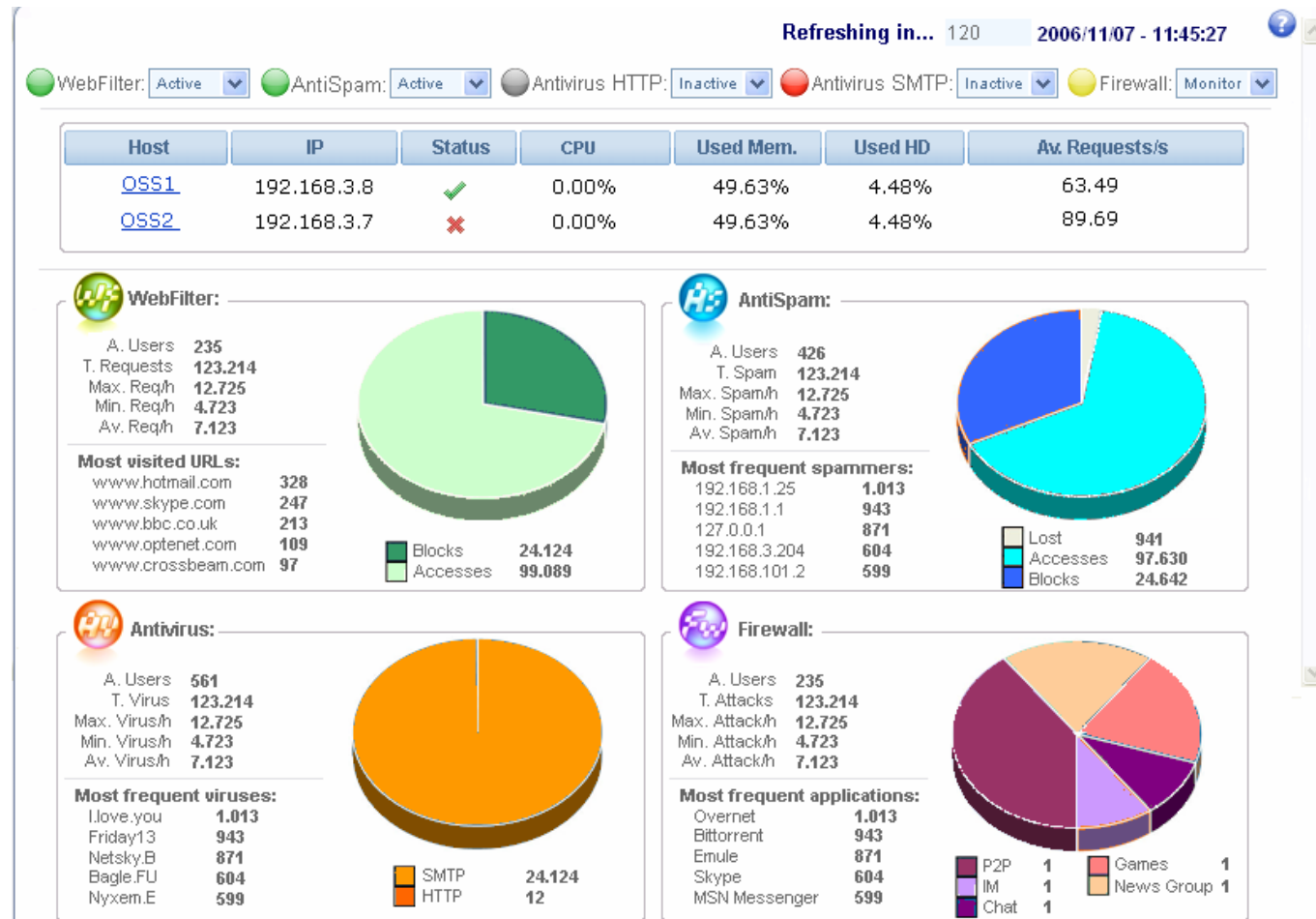
Enabled Target Group Profile Action Schedule

Enabled Optenet Madrid Active Categories Block Always

+34690172684  
+34690116290

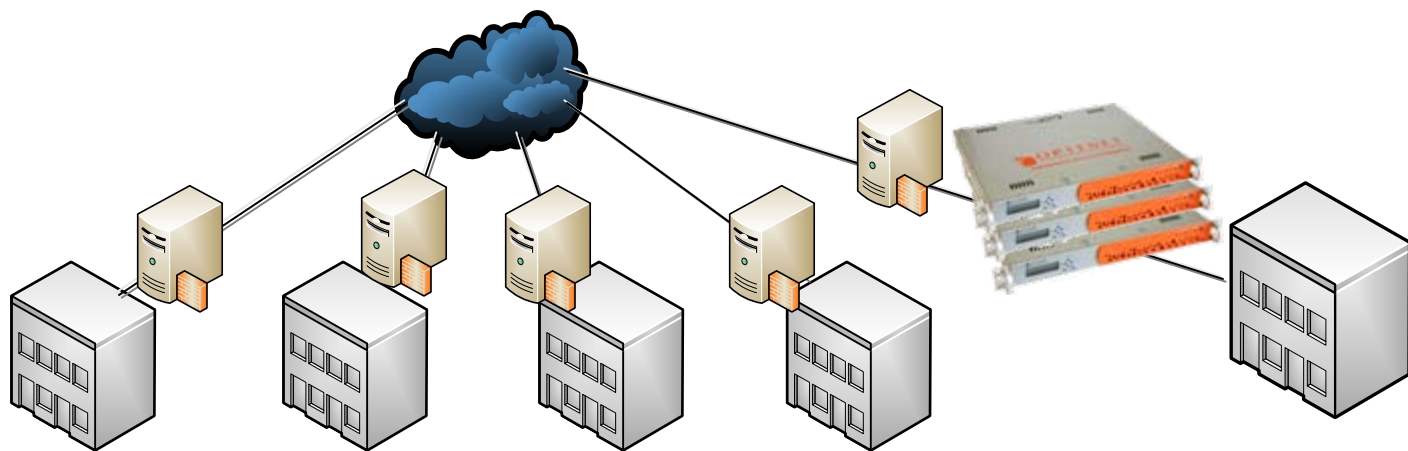
Banner Info Press Sport Selected Files

# Centralized Enterprise Reporting



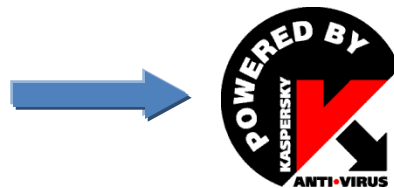
# Centralized Management

- Multi-branch security administration
  - Multi authentication: verifying identifiers
  - Multi administrators
  - Real cluster multi-appliance



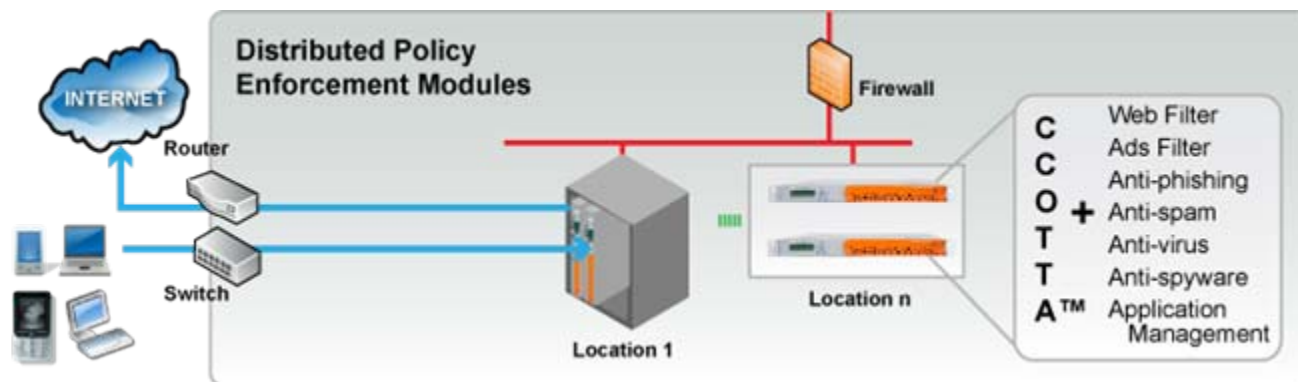
# Consolidated, Integrated Security

- Bidirectional, complete malware detection and filtering
  - Web content navigation
  - Adware
  - Phishing
  - Spyware
  - Virus
  - Spam
  - Application Management
  - Bandwidth Management



# Content Classification

- CCOTTA™
  - Carrier Class Optenet Transparent Traffic Analyzer
    - Intelligent management engine capable of bidirectional **L2 through L7** network traffic inspection across all protocols and ports
    - Reports network statistics in real time
- 24 x 7 research staff
- Access to third-party databases and tools



# Customer Case Study



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

## Bundesamt für Informatik und Telekommunikation

# The Challenge



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

## Objectives:

- Provide security services for 40 institutions and 40,000 end users
- Enforce basic security policy for all institutions
- Manage each institutions' security policies and LDAP sources for their users and groups.


## Requirements:

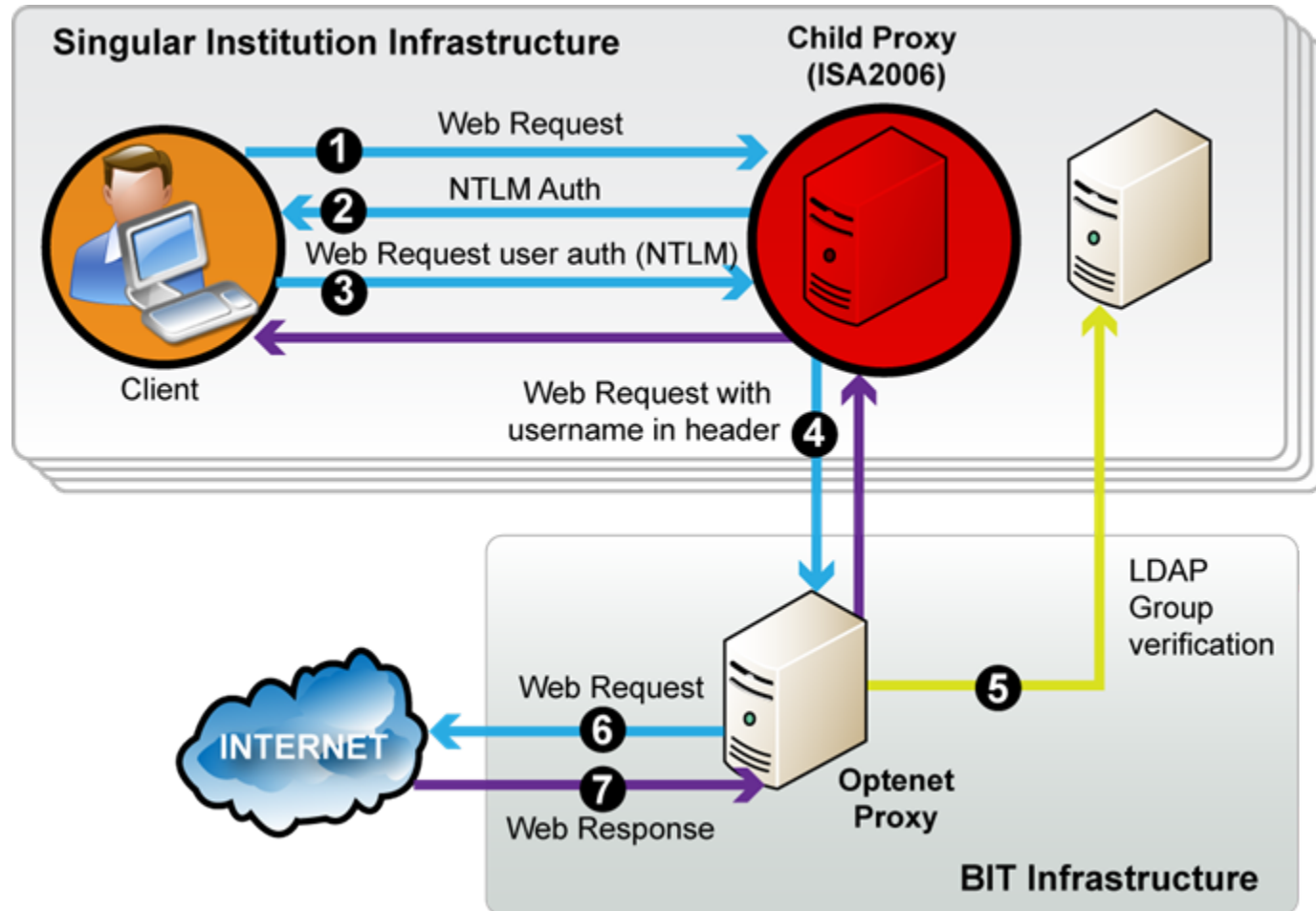
- Applications
  - Web filter
  - Antivirus
  - Protocol filter
  - Bandwidth management
- Architecture
  - Proxy environment

# Optenet Solution

- Multi-branch structure
- Deployment that incorporated:
  - Proxy mode
  - Multi-client structure
  - Multi-LDAP
  - Multi-authentication
- Services in one single solution
- Management in one integrated console
- Reporting capabilities available to each administrator according to granted privileges
- Competitive OPEX scheme: service... all included

# Deployment Scheme


 Schweizerische Eidgenossenschaft  
 Confédération suisse  
 Confederazione Svizzera  
 Confederaziun svizra



# Summary

- Optenet provides a new approach to implementing a content security solution for today and tomorrow
  - Distributed architecture ideally suited for in-the-cloud deployments
  - Dedicated team of researchers and partnerships with industry leaders
  - Highly scalable categorization engine to pre-process content
  - Integrates all major content security protections with ability to plug-in new modules
  - Complete and tightly integrated management console

# Thank you!

Questions? Stay tuned for the Q & A.

For more information on Optenet, please contact:

Joel Silberman, VP of North America

[jsilberman@optenet.com](mailto:jsilberman@optenet.com)

Or call Optenet's North American headquarters

1-800-250-9689