Cisco Expo 2008

# Jumping The Content Security Train

## Continuing the lead in L7 security

**Hrvoje Dogan**
**Systems Engineer, Eastern Europe and Russia**

IronPort Systems – A Cisco Business Unit

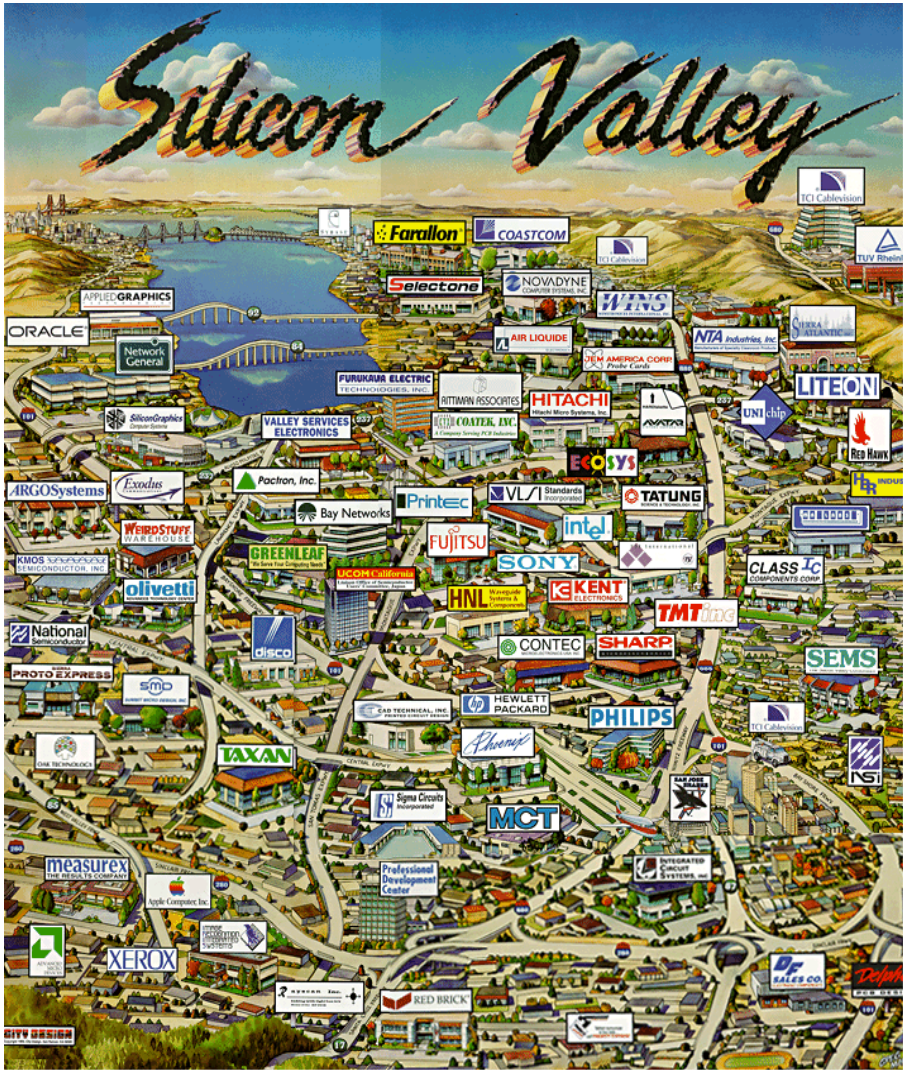
  

# Agenda

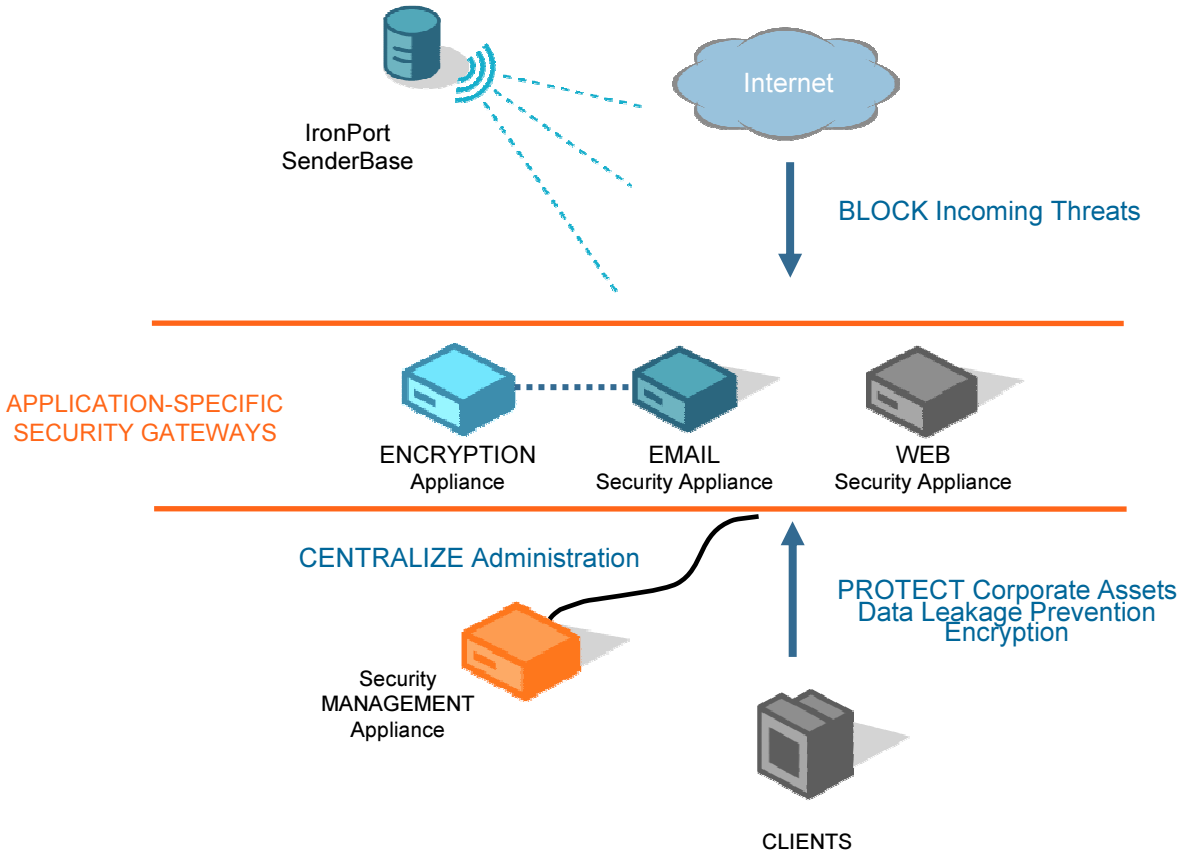
1. About IronPort
2. Market Position And Products Overview
3. Why did Cisco do it?
4. What do we do?
5. What can we do together?

# Who Is IronPort?

- Founded in 2000 by Email pioneers from Hotmail, ListBot and Yahoo
- idea: building the fastest and strongest gateway appliance
- based in USA, California, Silicon Valley
- Acquired by Cisco in June 2007
- Worldwide 800+ employees
- ~100 in Europe (UK, Germany, Sweden, France, Spain, Italy)
- revenue 2005: ~ 70m USD,
  2006: ~115m USD
  2007: ~200m USD



# IronPort® Gateway Security Products




Web Security | Email Security | Security Management | Encryption

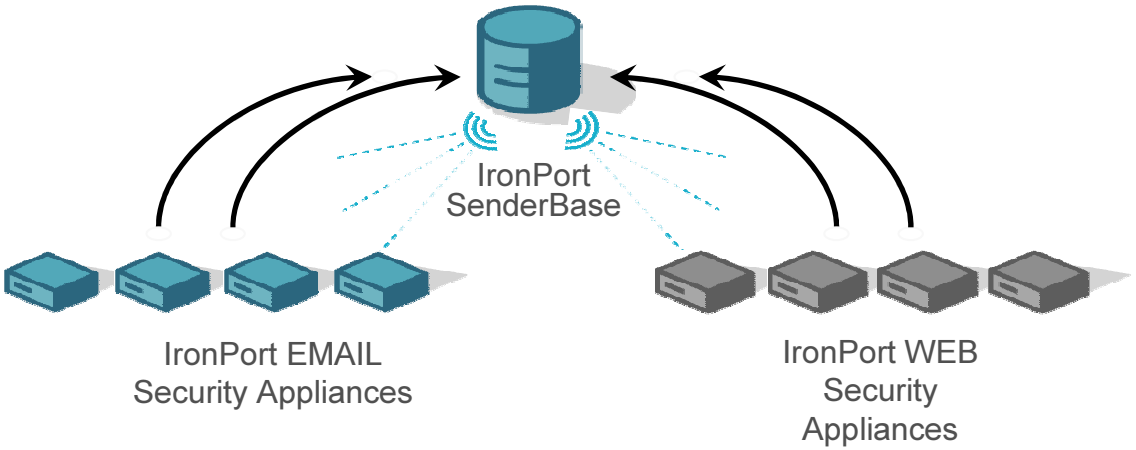
# The IronPort SenderBase® Network

*Global Reach Yields Benchmark Accuracy*

- 30B+ queries daily
- 150+ Email and Web parameters
- 30% of the World's Traffic
- Cisco Network Devices

- View into both Email & Web traffic
- 80% of spam contains URLs
- Email is a key distribution vector for Web-based malware
- Malware is a key distribution vector for Spam zombie infections

Combines Email & Web Traffic Analysis




*Source: www.securecomputing.com and www.borderware.com, August 6, 2006*

# IronPort + Cisco

## *Extending Market Leadership*


1. Customer Leadership

   Over 6,000 customers globally

   99% customer retention rate

2. Technology Leadership

   Industry leading email and Web security applications and management tools

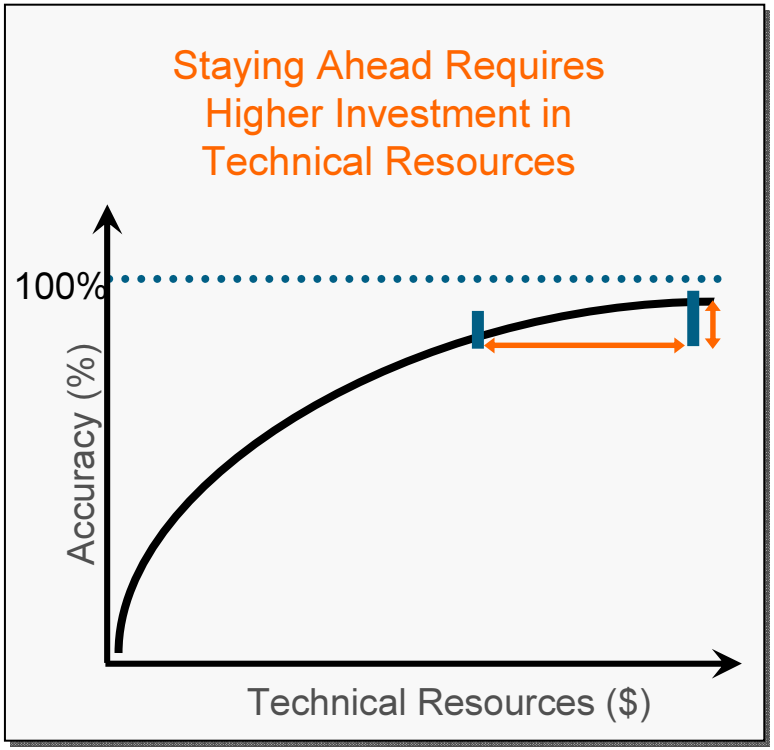
3. Global Leadership

   Worldwide operations and infrastructure

# IronPort + Cisco

*Extending Technology Leadership*

1. Substantial growth in bookings
   - Market growth rate = 50%
   - IronPort growth rate = 100%
2. Significant investment in security technology
   - R&D resources increased by 35% in 2007
   - Employee base increased by 50%
3. Unparalleled access to data
   - Cisco network devices contribute to IronPort's SenderBase data



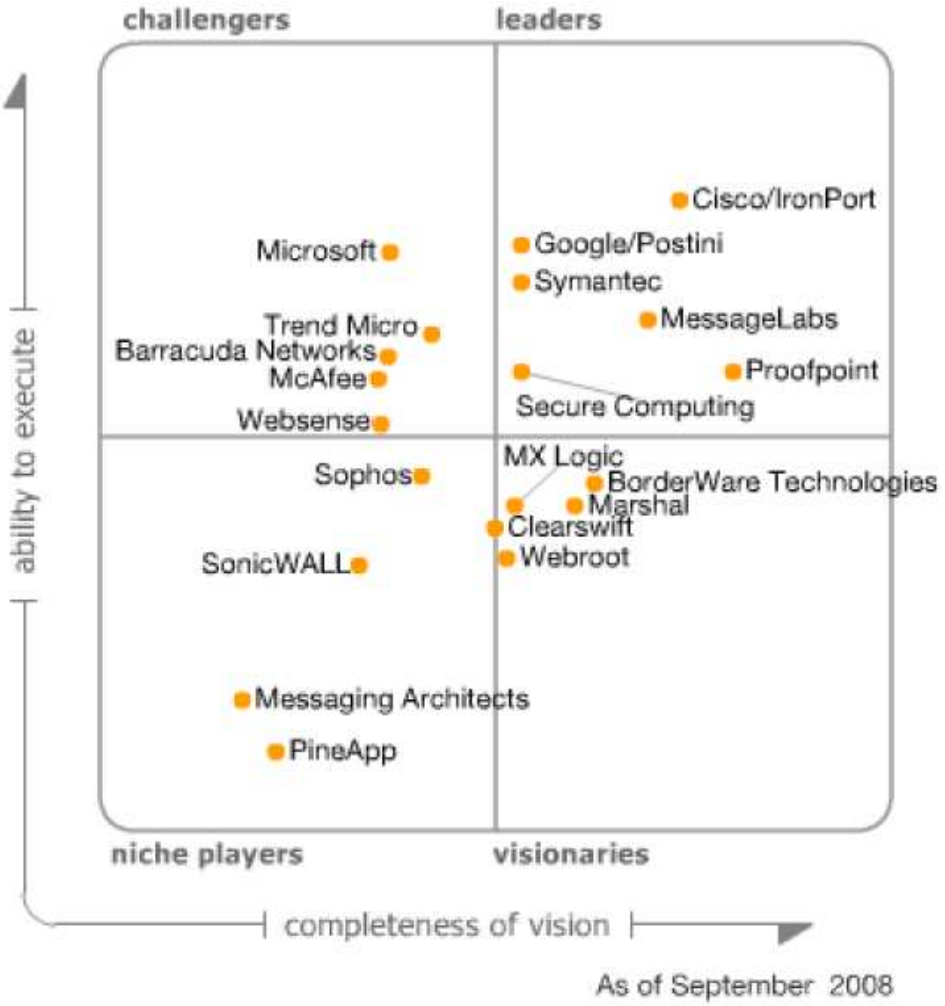

IRONPORT

# Gartner Magic Quadrant

*for Email Security Boundaries, 2008**

## Analysis of IronPort Email Security:

- Cisco/IronPort is the market share leader with strong growth rates.
- Spam detection rates for IronPort are excellent, with very low false-positive rates.
- SenderBase has expanded to include Web URL reputation. The local connection management policy is very granular.
- Email encryption (via the Cisco/PostX envelope functionality) is provided in the email security appliance.
- Scalability and stability are prime differentiators. IronPort has a large percentage of very large enterprise customers.




**Source: Gartner (September 2008)**

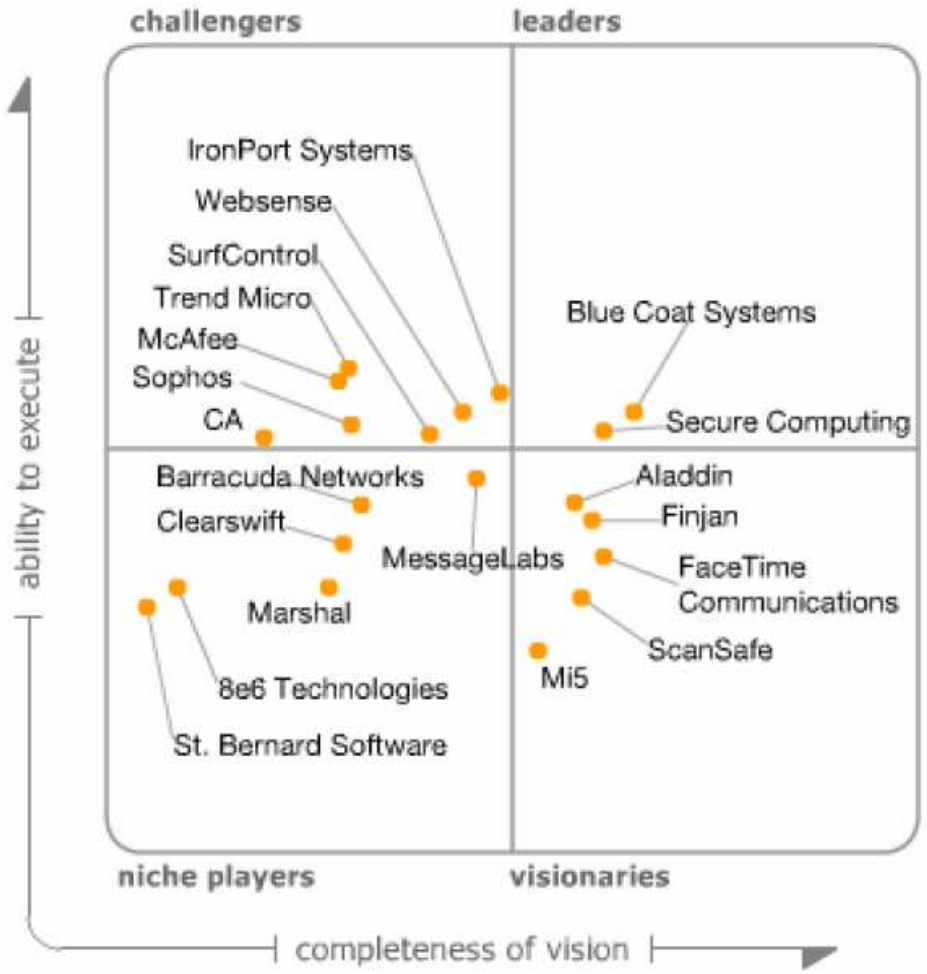
**Full report available on request.*

# Gartner Magic Quadrant

*for Secure Web Gateway, 2007**

## Analysis of IronPort Web Security:

- Email security experience has helped design the IronPort S-Series™ for complex enterprise environments.
- Solution provides anti-spyware scanning supplemented with anti-spyware scanning and URL filtering
- URL categorization engine is augmented with data from IronPort's SenderBase® reputation service.
- Malware protection is enhanced with an outbound Layer 4 traffic monitor
- IronPort is expected to be a leader in 2008 and potent threat as the product and installed base matures, and the company can take advantage of the reach of Cisco's sales force.




Source: Gartner (June 2007)

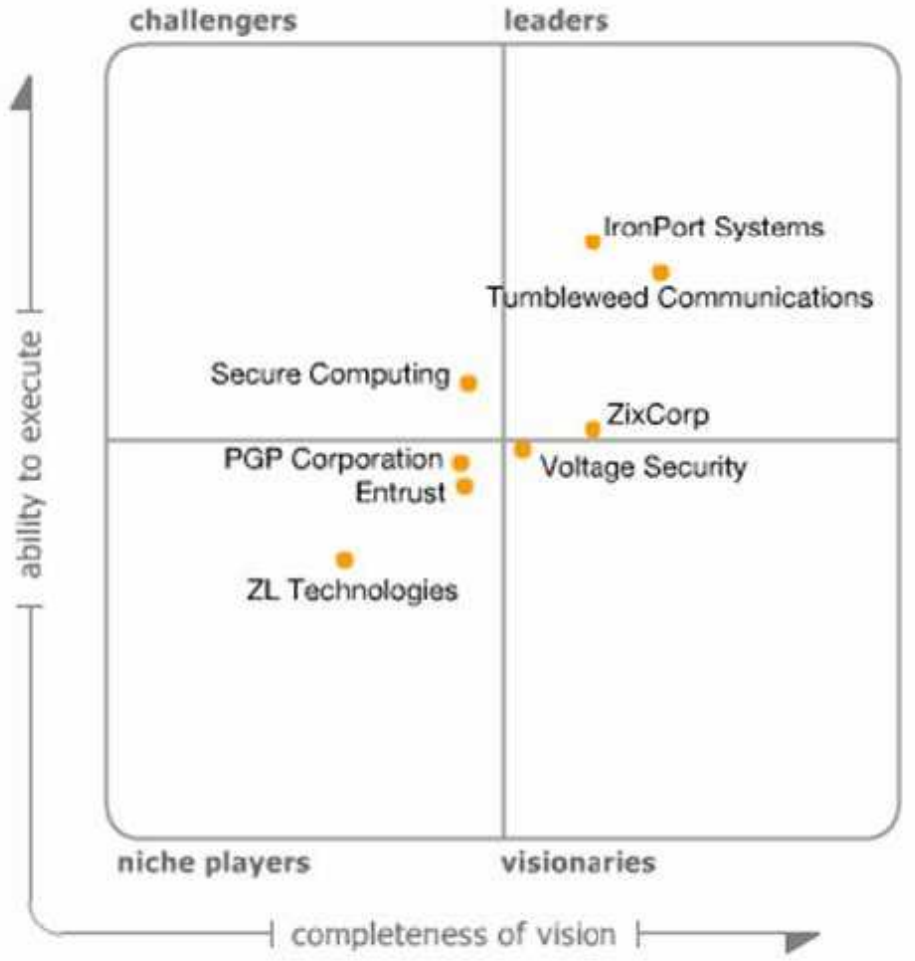
*Full report available on request.

# Gartner Magic Quadrant

*for Email Encryption, 2007**

## Analysis of IronPort Email Encryption:

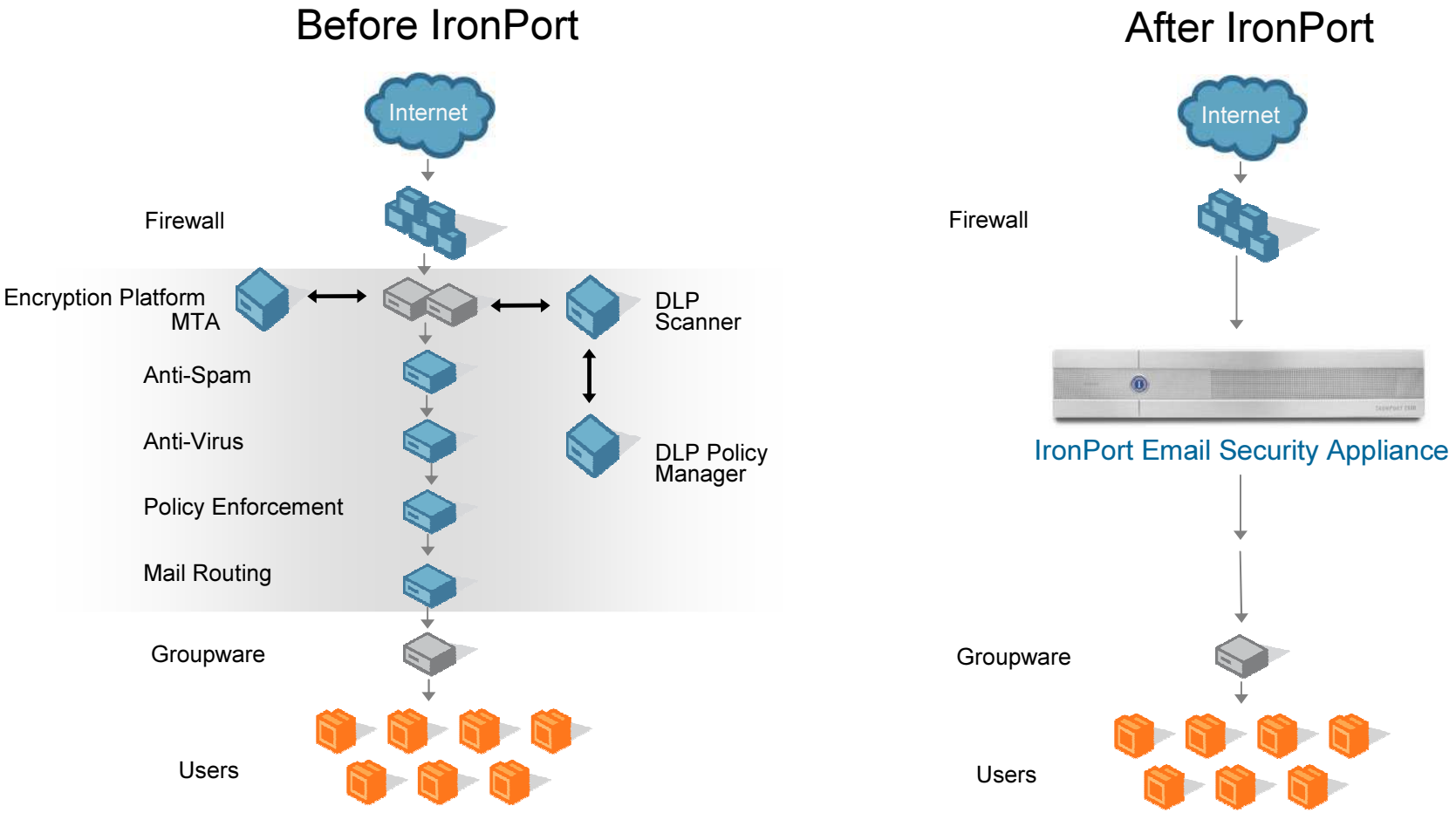
- Universal Reach: send to any email user
- Usability: No desktop software, no certificates
- Simple Deployment and Management
  - Integrated into IronPort C-Series™
  - Supporting infrastructure provided by Cisco-managed service
- Auditable Policy Enforcement
- Combined IronPort/PostX organization provides email security and encryption capabilities




*Full report available on request.

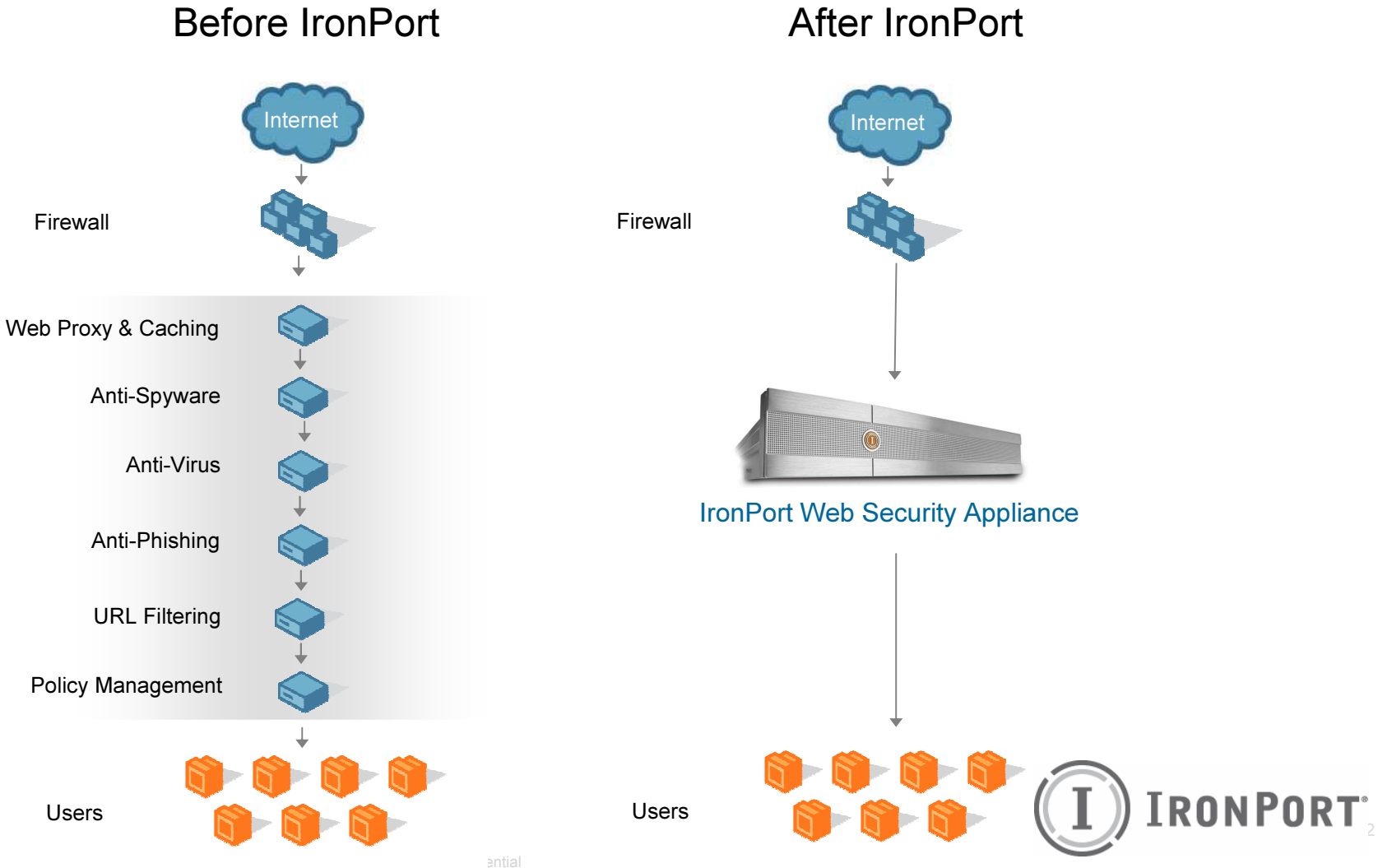
# IronPort Consolidates the Network Perimeter

*For Security, Reliability and Lower Maintenance*



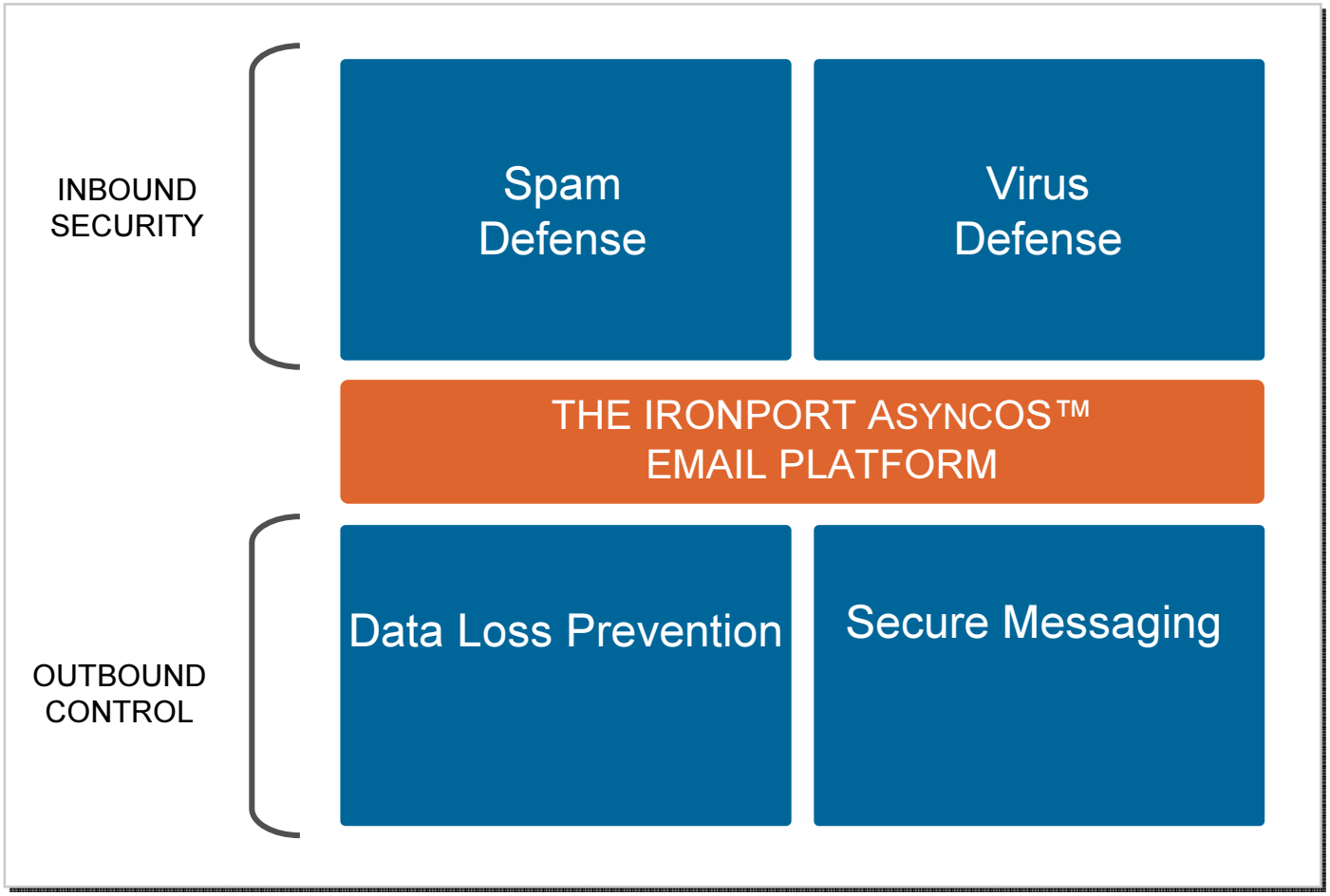
# IronPort Consolidates the Network Perimeter

*For Security, Reliability and Lower Maintenance*



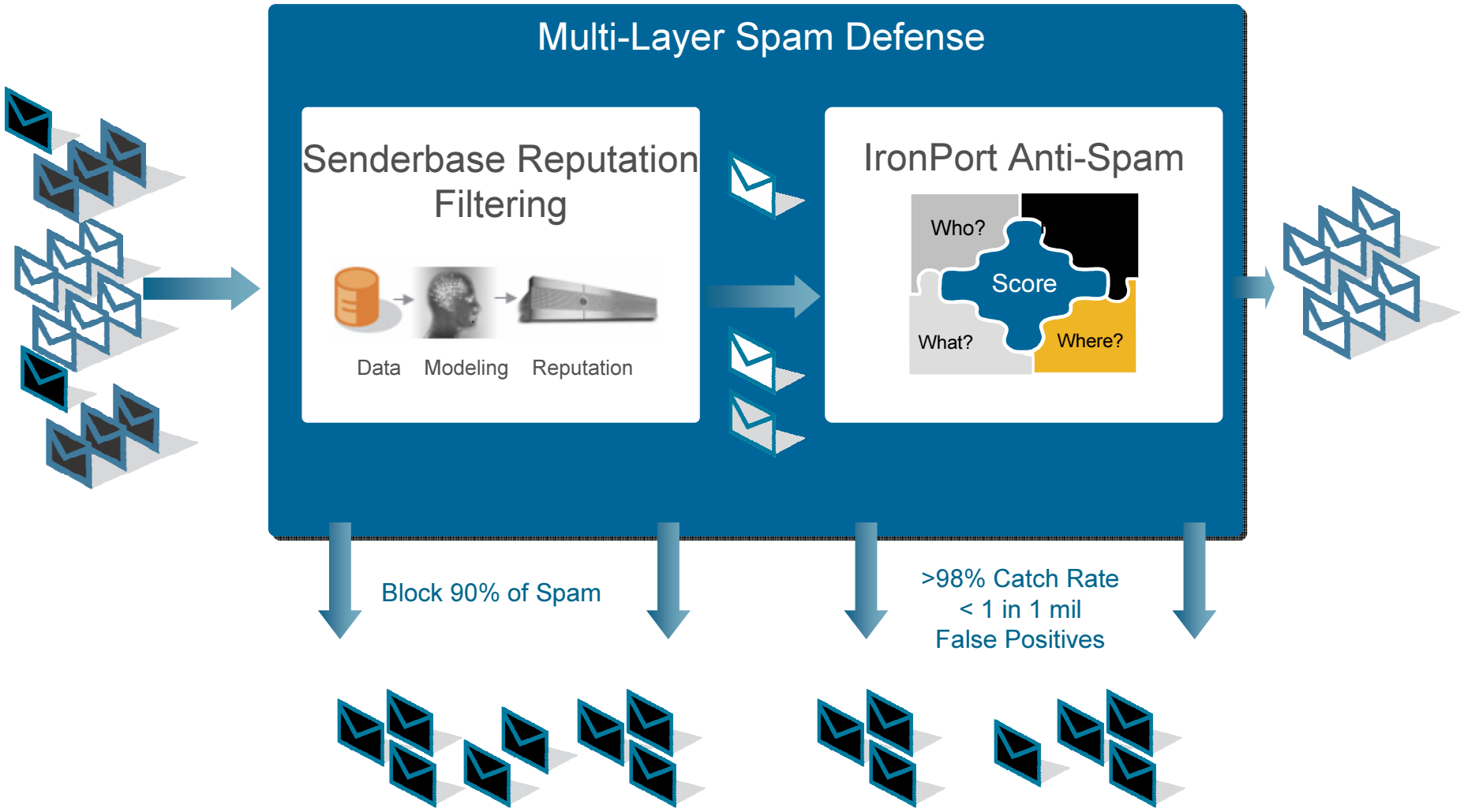
# IronPort E-Mail Security Architecture

*Inbound Security, Outbound Control*

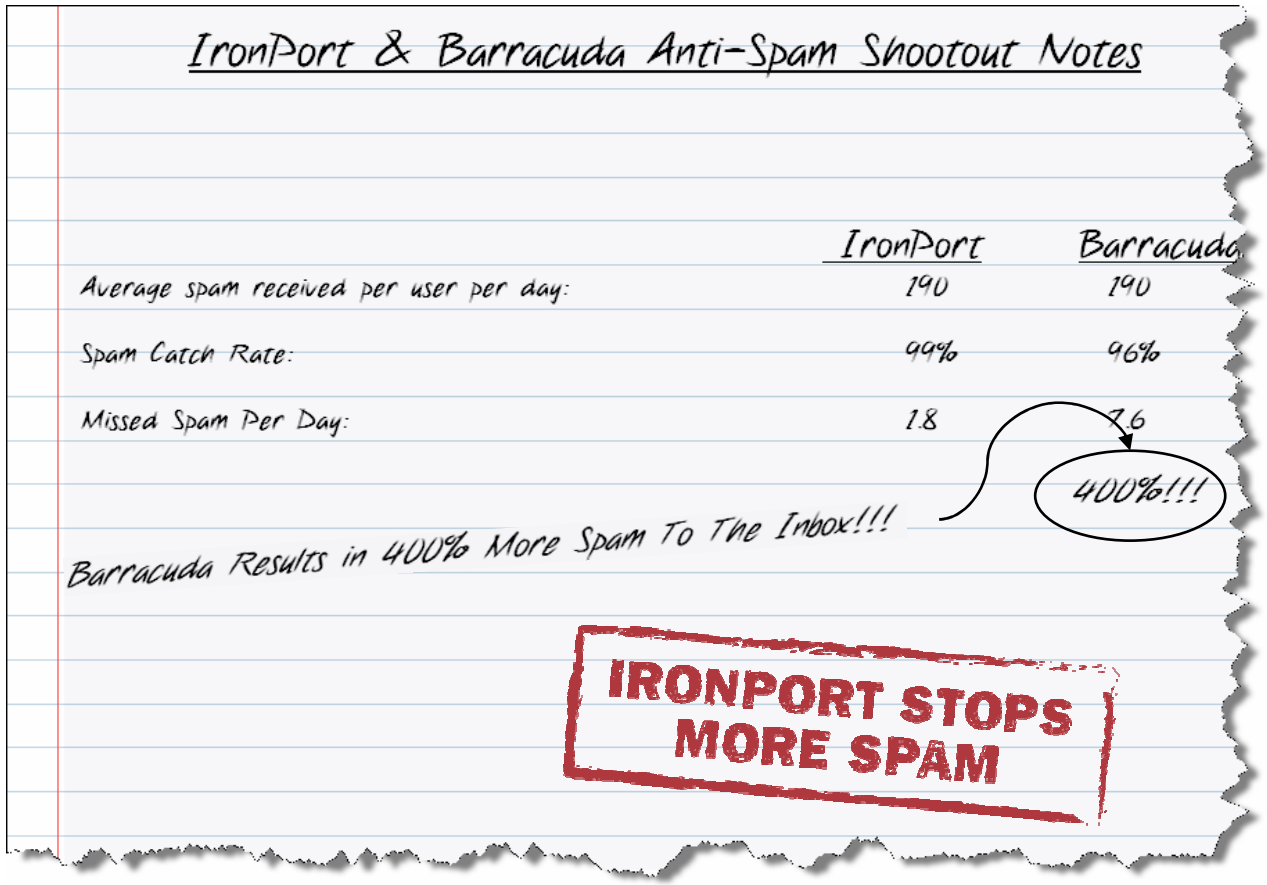


# Stop More Spam

*IronPort Spam Defense*



# IronPort Spam Defense
## *Thompson Machinery Case Study*




Thompson

*"I simply plugged it in, set it up and walked away. No more spam problems! The ROI on this product is a no-brainer."*

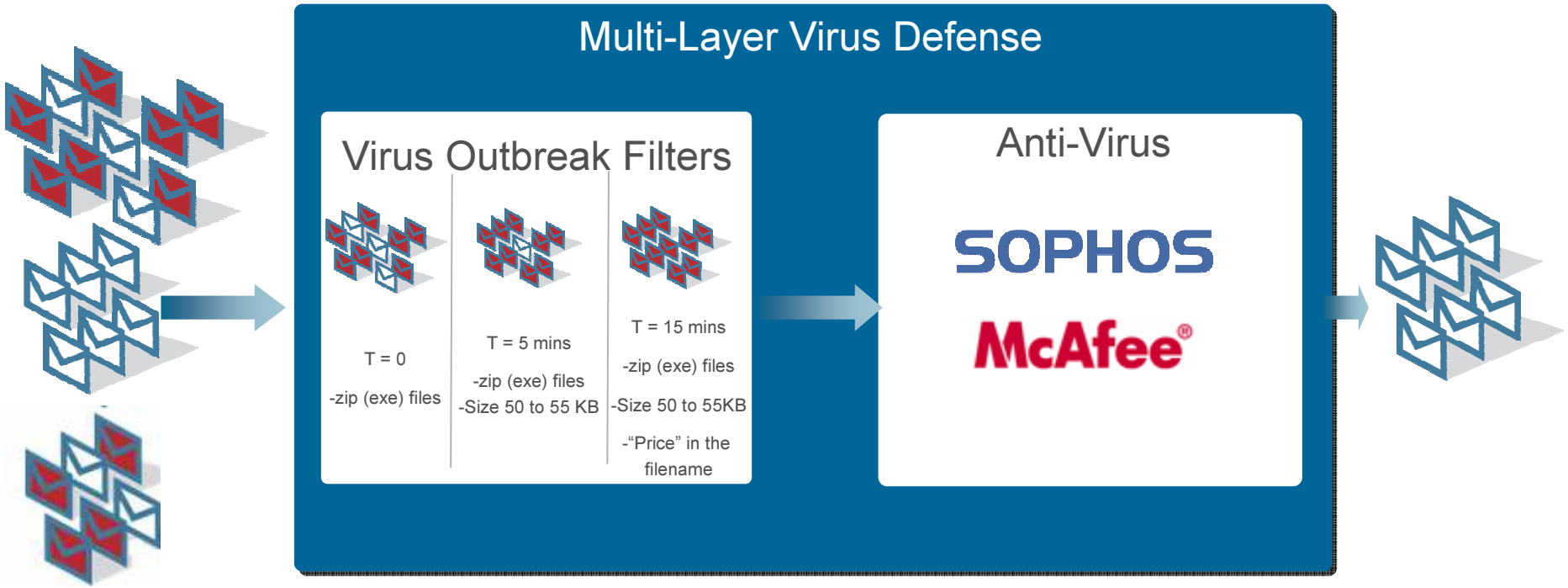
— David Jones
IT Administrator

Thompson Machinery

| MAILBOXES PROTECTED | 500+ |
|---|---|

# Stop More Viruses

*IronPort Virus Defense*



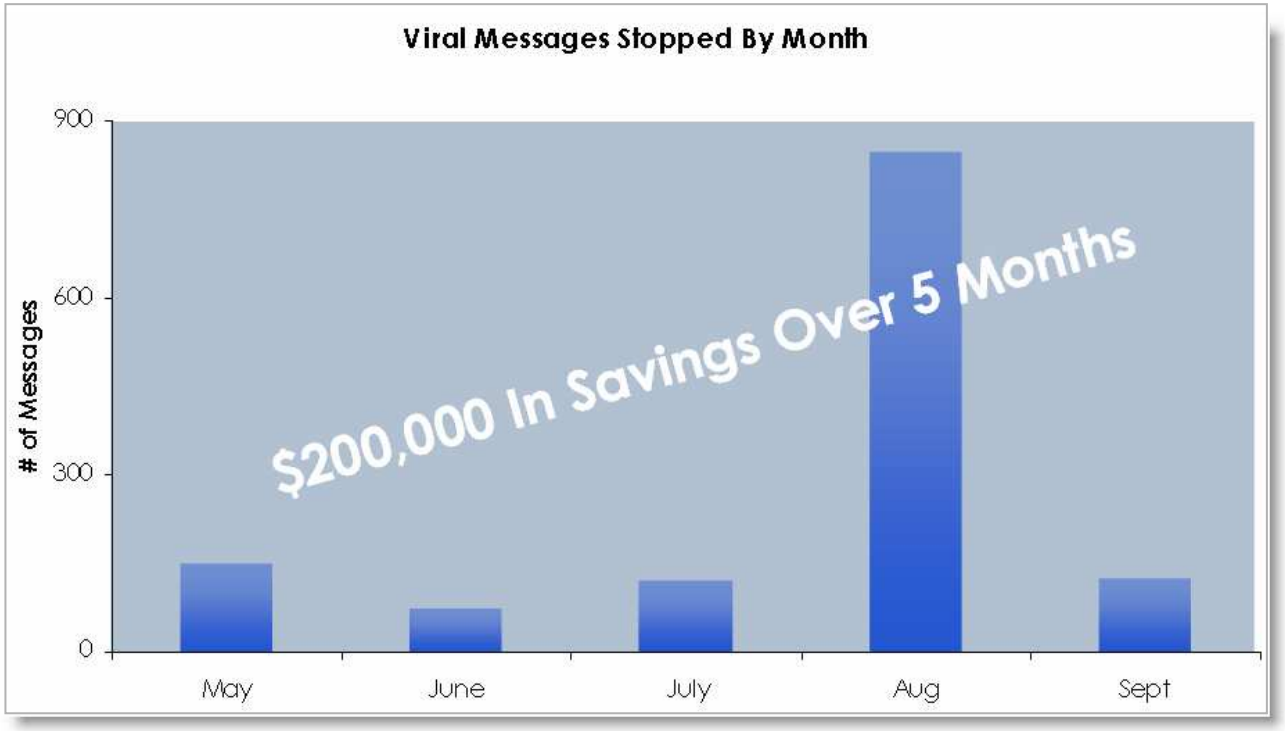

Virus Outbreak Filters Advantage

Average lead time*……over 13 hours

Outbreaks blocked * ……175 outbreaks

Total incremental protection*……over 94 days

# IronPort's Virus Defense
## *eWeek Review Case Study*




*Assumes $500 Per Desk Top Clean Up & 1/3 Open Rate of Viral Messages*

eWEEK

### Review

- 5 month test by eWEEK
- 1217 virus positive emails stopped before AV signatures were available
- 48 separate virus variants
- 0 false positives reported

*"We never saw a false positive. Virus Outbreak Filters effectively blocked messages containing viruses for which signatures didn't already exist."*

— - Mike Caton, Technical Writer

# Data Loss Prevention

*Multi-Faceted Problem*

1. Regulatory Compliance

   PCI, HIPAA, GLB, SOX Regulations

   Scan for sensitive information and block infractions

   Secure business partner communication

2. Acceptable Use

   Block offensive content

   Enforce messaging policy (attachment size, etc)

   Add legal disclaimers to outgoing mails

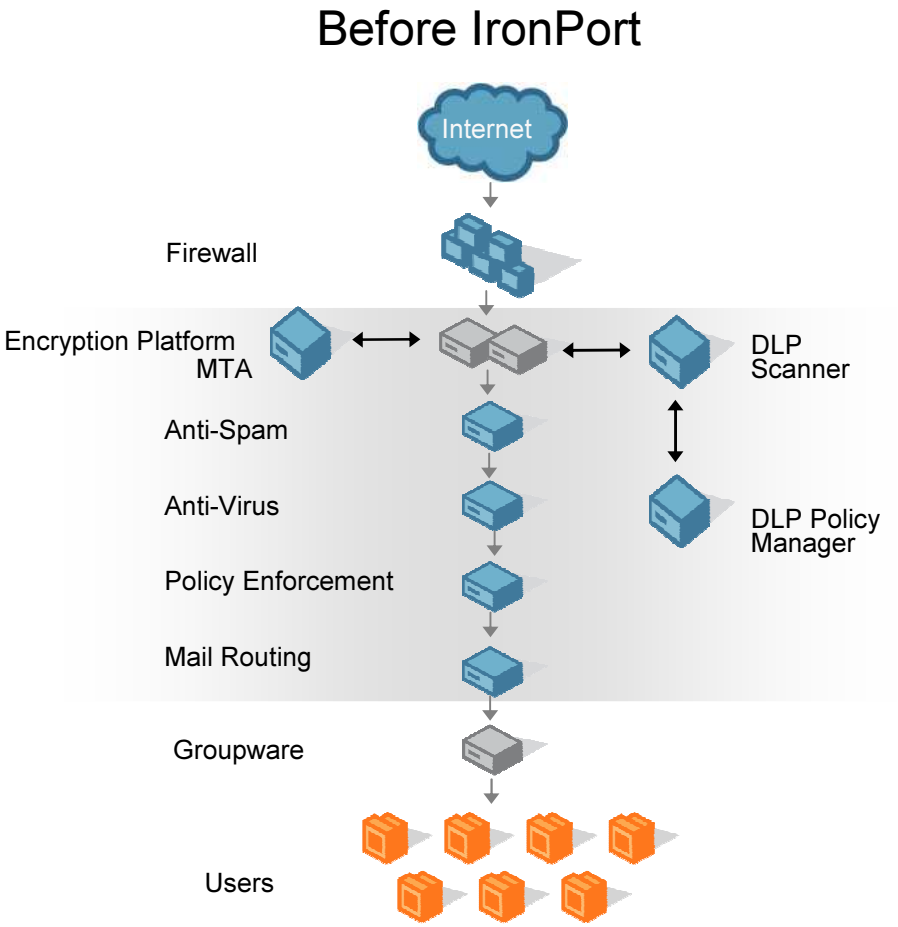
3. Intellectual Property Protection

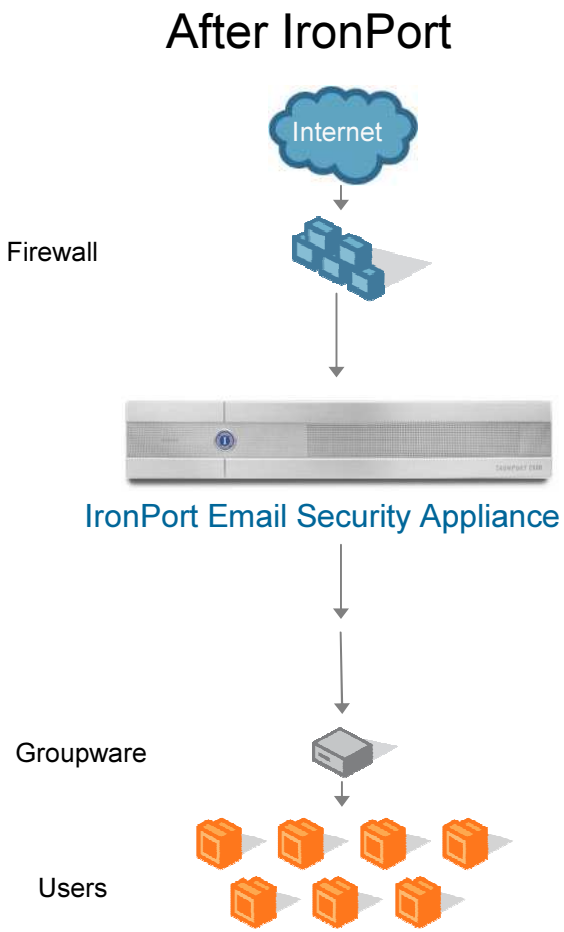
   Block messages containing confidential data

   Prevent email communications with competitor

# Data Loss Prevention Deployment

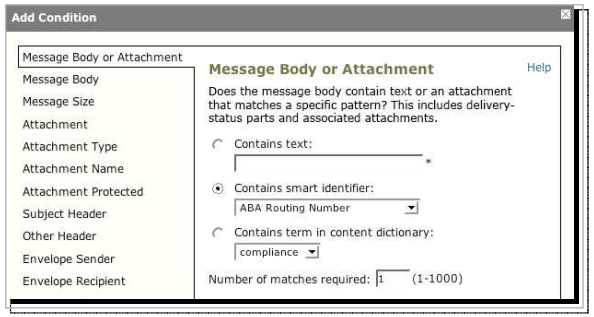
*IronPort Reduces Complexity*



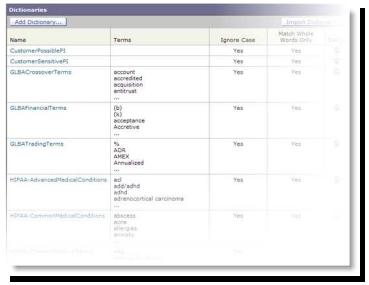



# Data Loss Prevention Foundation

*Integrated Scanning*

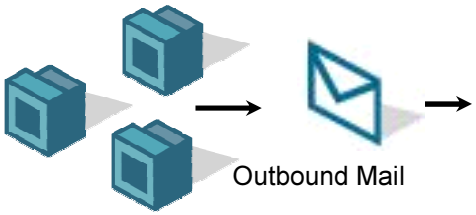


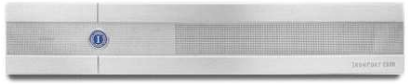

Custom Content Filters

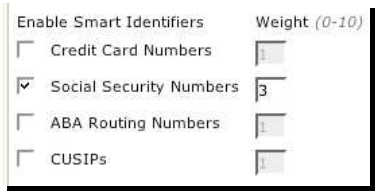


Compliance Dictionaries

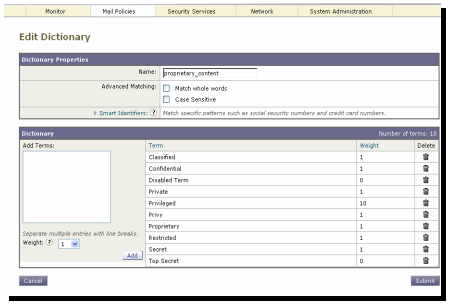
Users



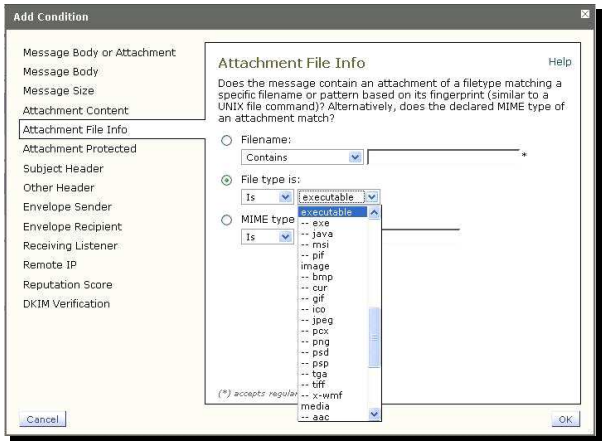






Smart Identifiers




Weighted Content Dictionaries

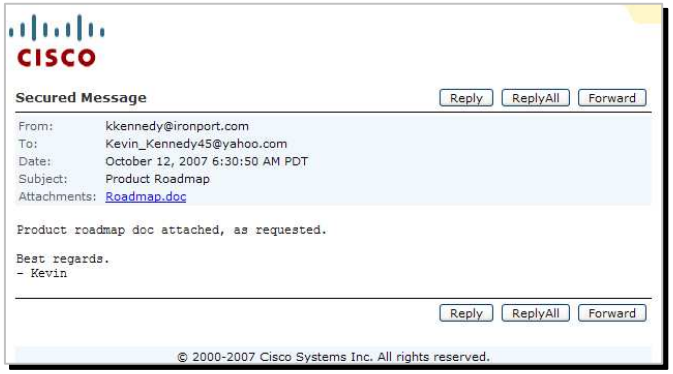



Attachment Scanning

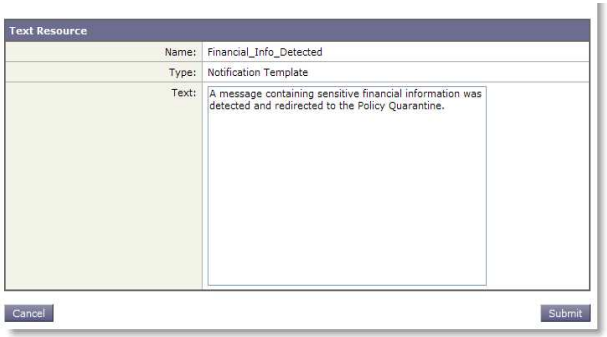
*Integrated Scanning Makes DLP Deployments Quick & Easy*

# Data Loss Prevention Foundation

## *Integrated Remediation*

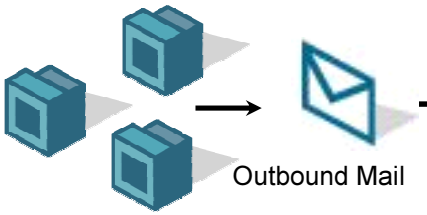



Remediation: Encryption

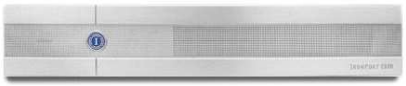


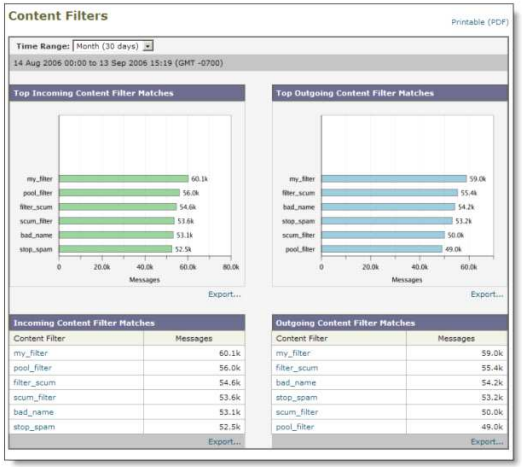

Remediation: Notification

Users

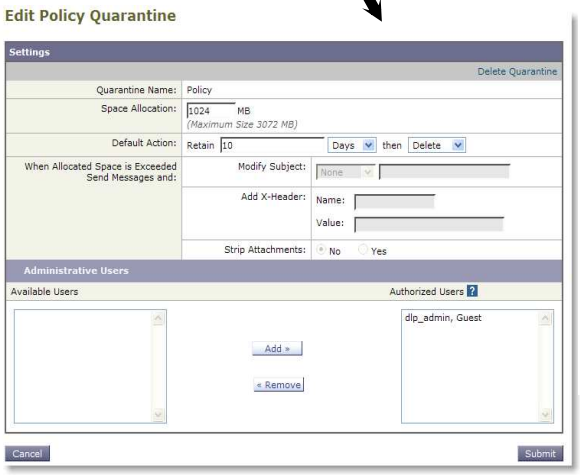


Outbound Mail






Remediation: Reporting




Remediation: Quarantine

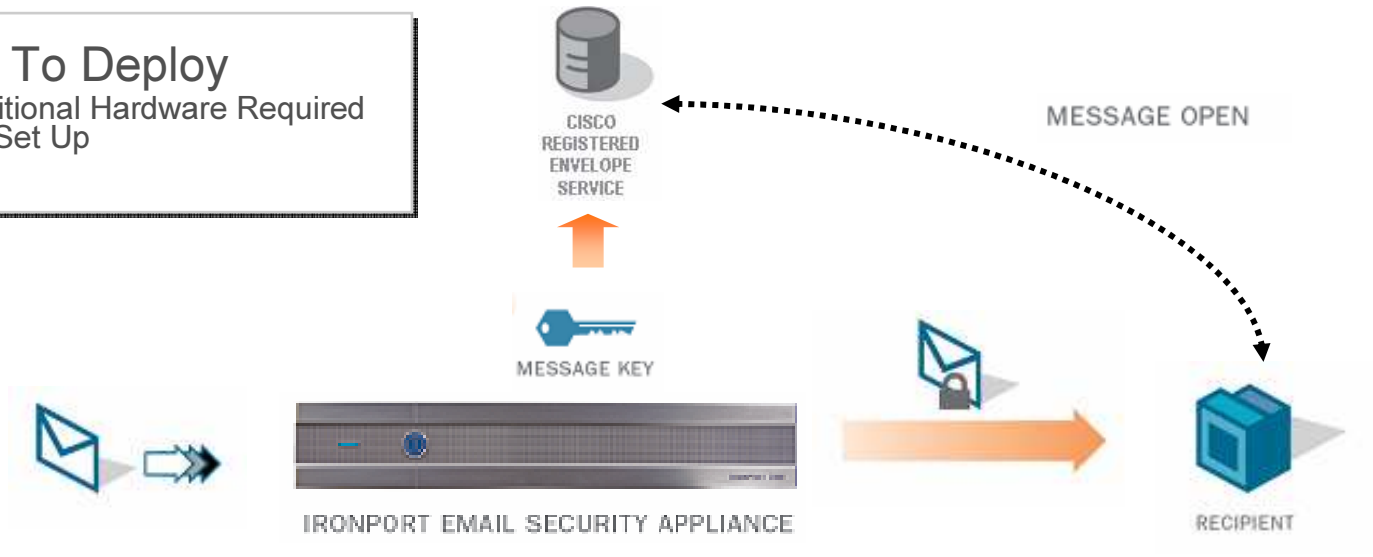
*Integrated Remediation Eases Work Flow Burden*

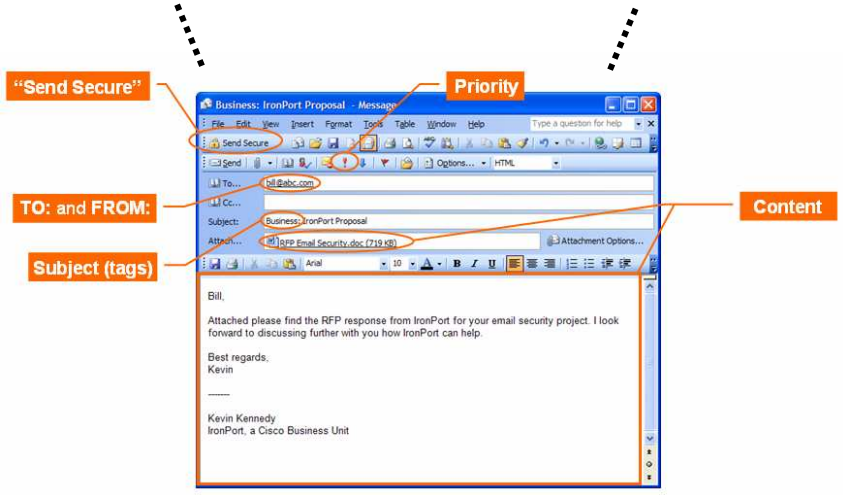
# Secure Messaging

## *Email Encryption That's Easy For Senders*

### Easy To Deploy

No Additional Hardware Required
3 Step Set Up



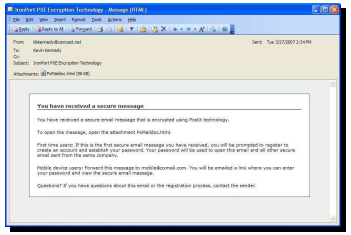

### Easy Policy Assignment

Central Policies
User-Driven Policies

# Secure Messaging

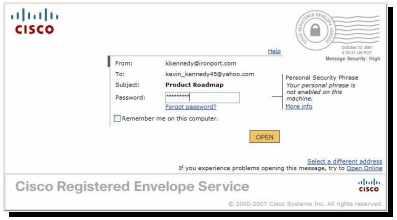
*Email Encryption That's Easy For Receivers*

## 1. Open Attachment

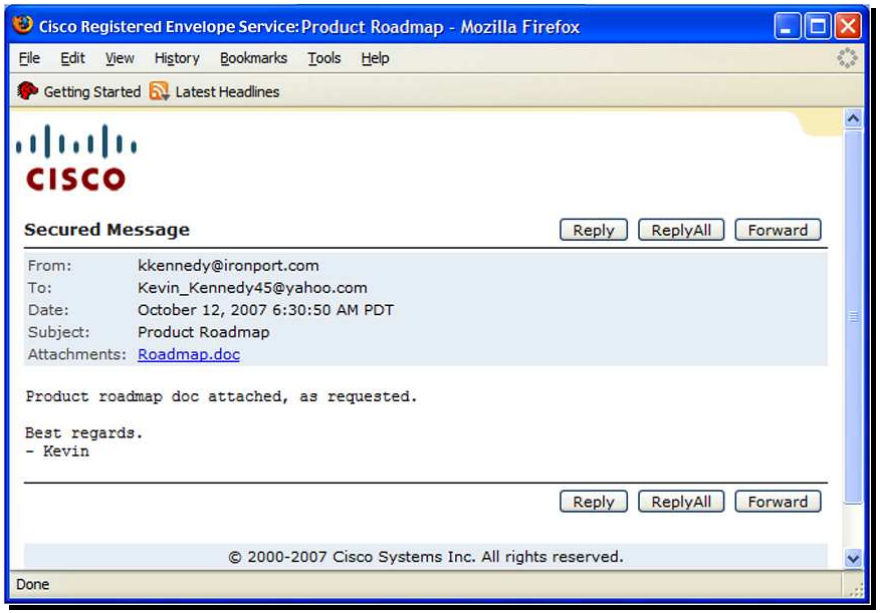


Send To Anyone
No Certificates
No Plug-Ins

## 2. Enter password

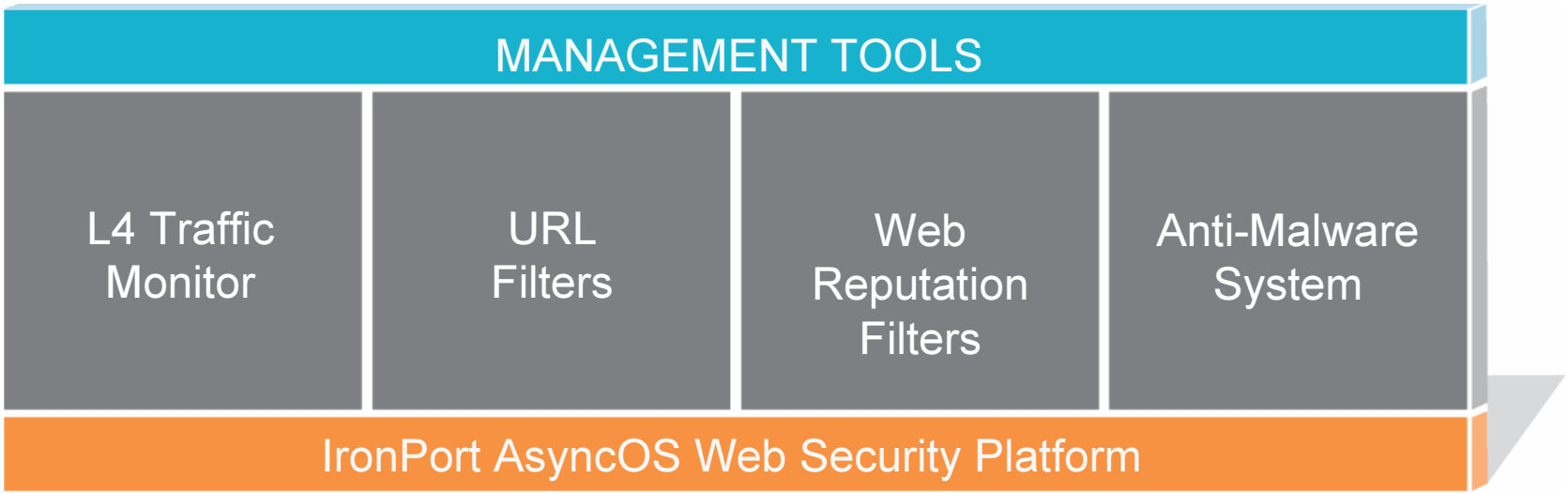



## 3. View message



# IronPort Web Security Architecture

*The Next Generation Secure Web Gateway*




IRONPORT

# Detecting Existing Client Infections

*Monitoring "Phone Home" Traffic*

1. Layer 4 Traffic Monitor

   Scans all traffic, all ports, all protocols

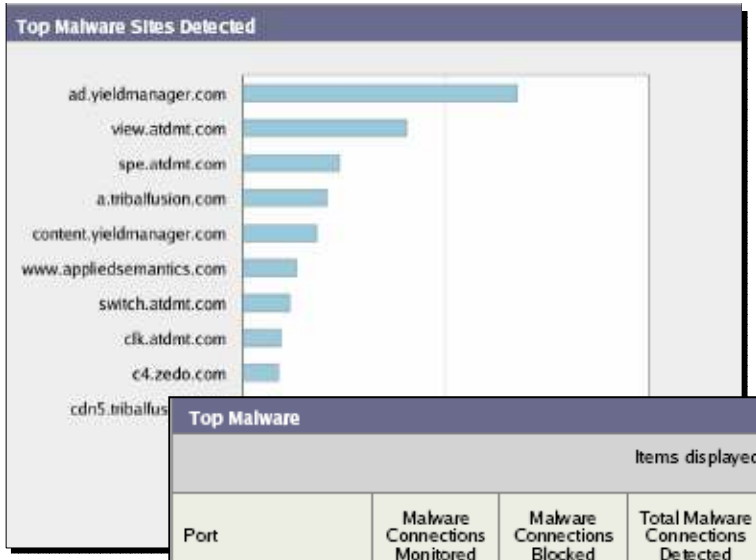
   Detects malware bypassing

   Port 80

2. Powerful anti-malware data

   Automatically updated anti-malware rules

   Real-time rule generation using "Dynamic Discovery"




**Top Malware**

Items displayed: 10

| Port | Malware Connections Monitored | Malware Connections Blocked | Total Malware Connections Detected |
|---|---|---|---|
| 80 | 1.2M | 0 | 1.2M |
| 443 | 17.9k | 0 | 17.9k |
| 1935 | 1,823 | 0 | 1,823 |
| port N/A | 949 | 0 | 949 |
| 28555 | 875 | 0 | 875 |
| 25 | 514 | 0 | 514 |
| 8080 | 336 | 0 | 336 |
| 53 | 258 | 0 | 258 |
| 81 | 113 | 0 | 113 |
| 8081 | 105 | 0 | 105 |

# IronPort Web Security
*Aurora Health Care Case Study*


## 1. Aurora Health Care's challenge:

13 Hospitals, 100 clinics, over 30,000 users

Significant malware infections

Large infrastructure, ~7 servers running Websense

## 2. IronPort's solution:

Blocked **~2 million** additional suspect transactions per week (downloads.hotbar.com, zedo.com)

Spyware filtering accuracy increased by **3x**

Replaced **7** servers with **2** IronPort S-Series™ appliances

Servers consolidated by **70%**

Aurora Health Care®

*"… we have been very concerned about the level of malware infections in our network. The fact that the IronPort S-Series enables us to stop malware at the network edge, while also allowing us to deploy URL filtering policies, is a big advantage for us."*

— Tim Sommers
AURORA HEALTH CARE

| USERS PROTECTED | 30,000+ |
|---|---|

# IronPort URL Filters

## *Leading Accuracy and Control*

- Enterprise-class database

  52 categories, over 21 million sites, ~3.5 billion webpages

  1/3 of the database is international

- 24 x 7 monitoring
- Regular, automated updates

| Categories |
| --- |
| ***Advertisements & Pop-ups*** |
| ***Arts*** |
| ***Blogs & Forums*** |
| ***Business*** |
| ***Chat*** |
| ***Computing & Inte*** |
| ***Downloads*** |
| ***Education*** |
| ***Entertainment*** |
| ***Fashion & Beauty*** |
| ***Finance & Invest*** |
| ***Food & Dining*** |
| ***Games*** |
| ***Government*** |
| ***Health & Medicin*** |
| ***Hobbies & Recrea*** |
| ***Hosting Sites*** |

| Categories |
| --- |
| *Infrastructure* |
| *Intimate Apparel & Swimwear* |
| *Job Search & Career Development* |
| *Kids Sites* |
| *Motor Vehicles* |
| *News* |
| *Peer-to-Peer* |
| *Personals & Dating* |
| *Philanthropic & Professional Orgs.* |
| *Photo Searches* |
| *Politics* |
| *Proxies & Translators* |
| *Real Estate* |
| *Reference* |

# IronPort URL Filters

*Comprehensive Management & Visibility*

1. Flexible policy management
   - Per user, per group policies
   - Multiple actions, including monitor only
   - Custom notifications
2. Visibility
   - Easy to understand reports
   - Extensive logging
   - Comprehensive alerting

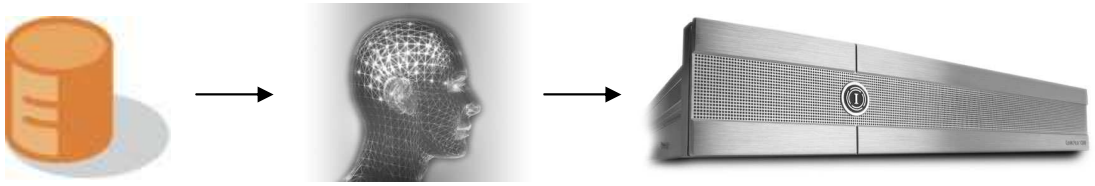
# IronPort Web Reputation Filters

*Data Makes the Difference*

## Parameters

- URL Blacklists
- URL Whitelists
- URL Categorization Data
- HTML Content Data
- URL Behavior
- Global Volume Data
- Domain Registrar Information
- Dynamic IP Addresses
- Compromised Host Lists
- Web Crawler Data
- Network Owners
- Known Threats URLs
- Offline data (F500, G2000…)
- Website History

THREAT PREVENTION IN REALTIME



SenderBase Data

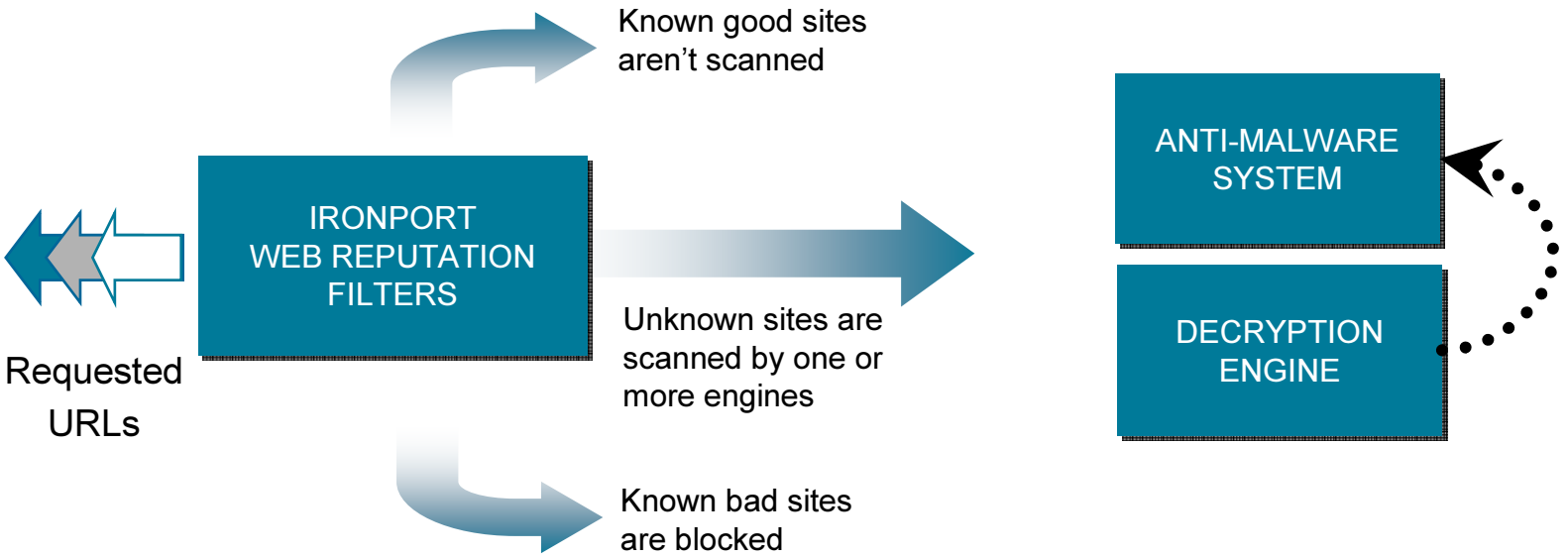
Data Analysis/ Security Modeling

Web Reputation Scores (WBRS) -10 to +10

*Addresses Known and Unknown Sites*

IRONPORT

# Intelligent Scanning



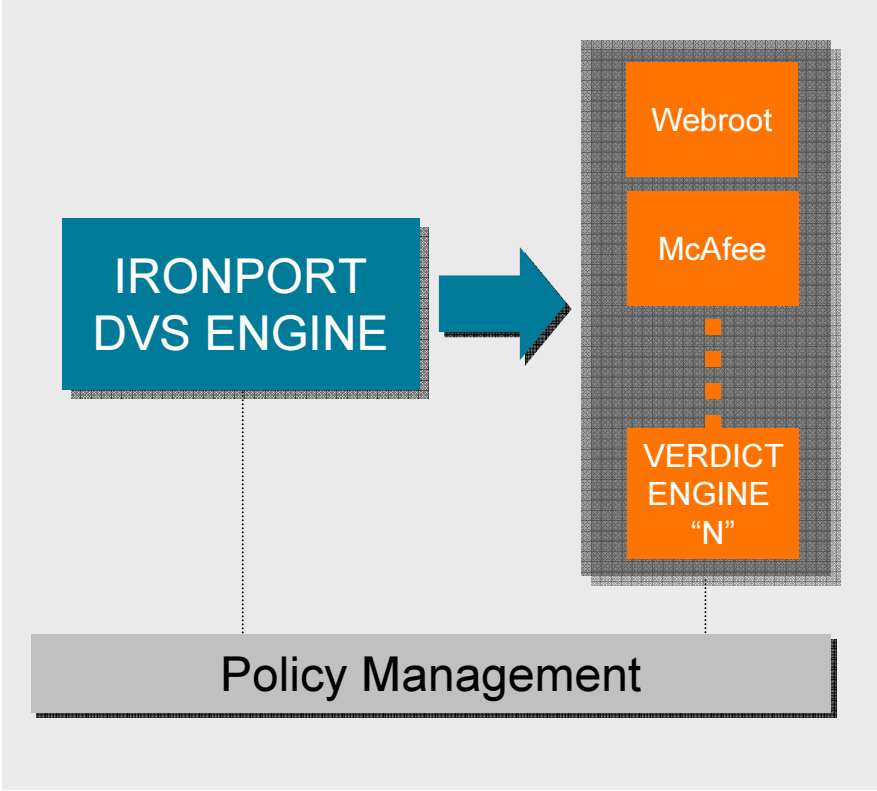

1. **IronPort Web Reputation** technology determines need for scanning by
   - IronPort Anti-Malware System™
   - Decryption Engine

IRONPORT®

# IronPort DVS Engine

*Multi-Layered Malware Defense*

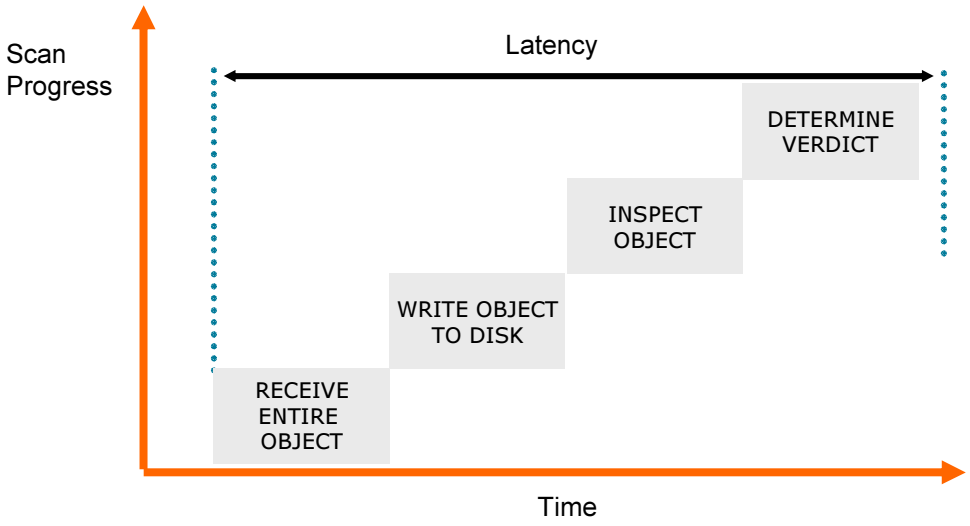
1. Deep content inspection
2. High-performance scanning
   - Parallel scans
   - Stream scanning
3. Multiple verdict engines
   - Integrated, on-box
   - Supported engines: Webroot, McAfee
4. Automated Updates

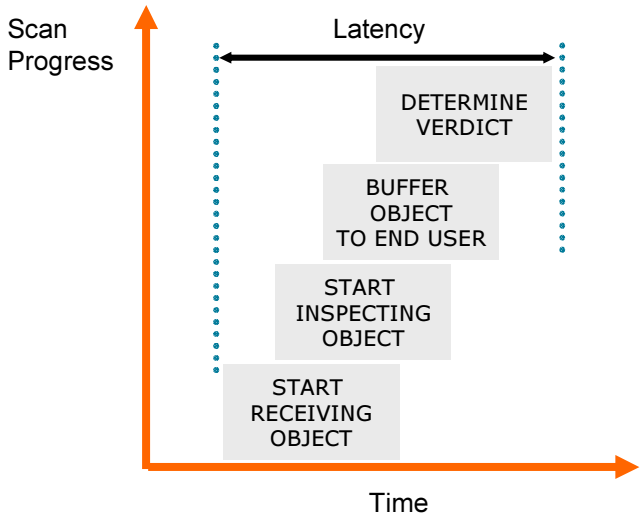



IRONPORT

# Industry Leading Performance

## *Stream Scanning*




1. Accurately identifies “safe” objects for stream scanning
2. Processes objects in parallel to minimize latency

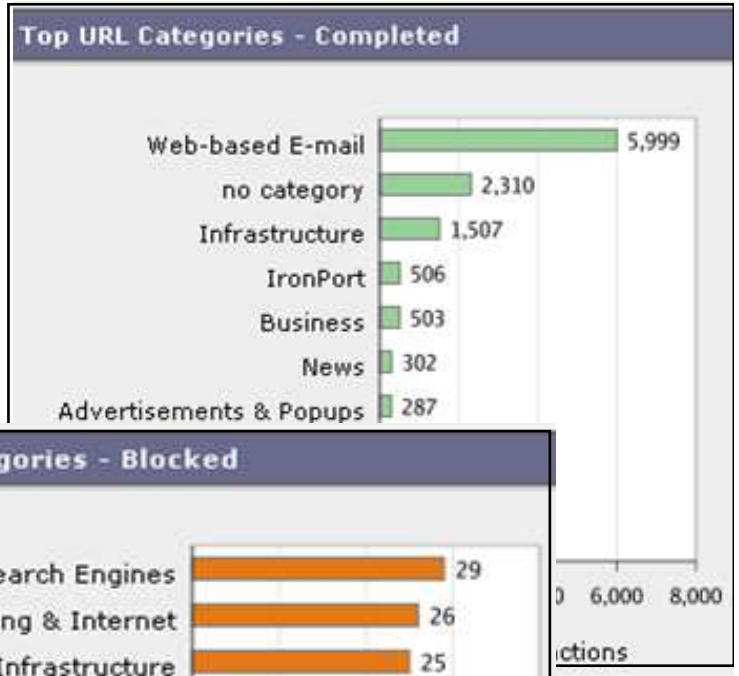
IRONPORT

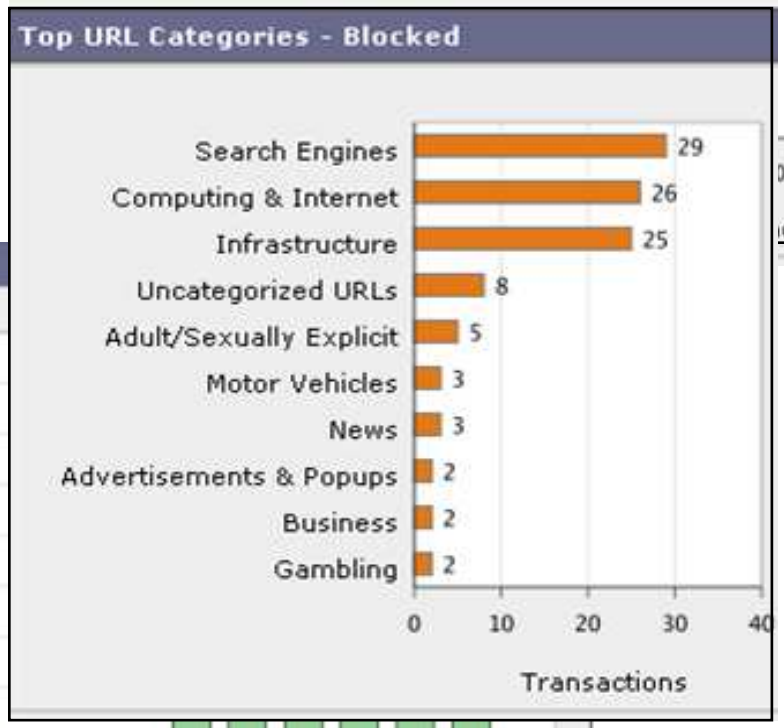
# Enforcing Acceptable Use

## *Customer Use Case*

Flexible acceptable use policies, with with easy-to-understand reporting

1. Track Work Force Productivity
2. Reduce Resource Consumption
3. Protect from Legal Liability




95% of companies who try an IronPort appliance become customers.

*Sales Contact:*
Mirko Schneider
*Territory Manager*

mschneider@ironport.com

IRONPORT

Cisco Expo 2008

# Thank You!

**Hrvoje Dogan**
**Systems Engineer, Eastern Europe and Russia**

IronPort Systems – A Cisco Business Unit

hdogan@ironport.com