IronPort Perimeter Security Appliances

EMAIL & WEB OVERVIEW

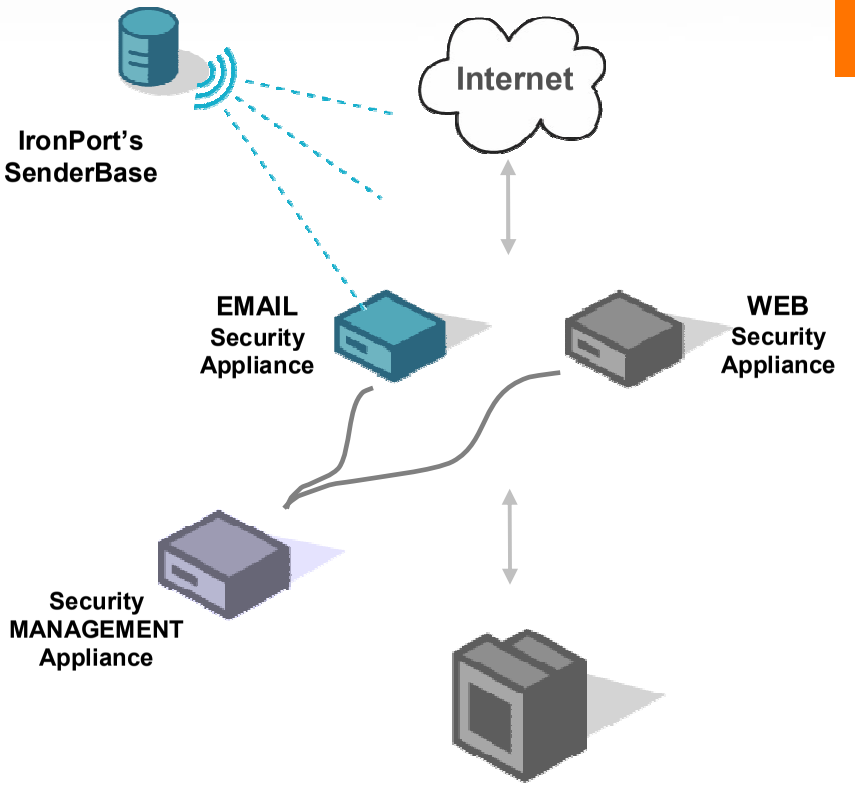
IronPort is now part of Cisco.

CISCO

IRONPORT

Email Security Overview

IronPort® Perimeter Security Appliances



Web Security | Email Security | Security management

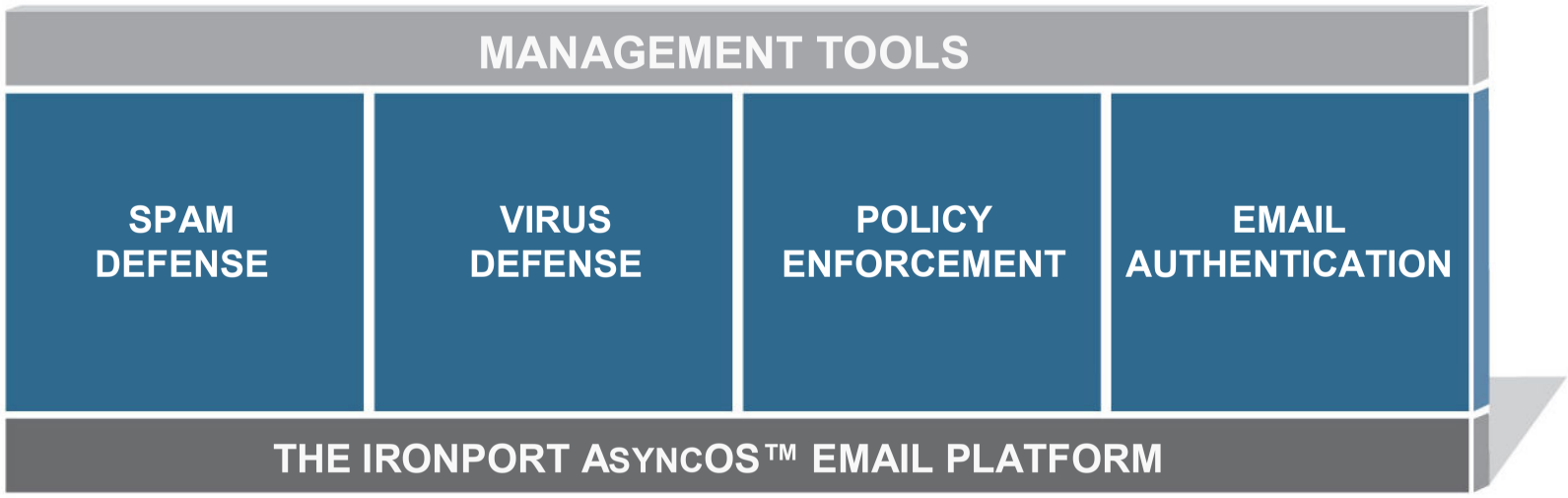
IRONPORT®

IronPort + Cisco

Extending Market Leadership

- **Customer Leadership**
  - Over 6,000 customers globally
  - 99% customer retention rate
- **Technology Leadership**
  - Industry leading email and Web security applications and management tools
- **Global Leadership**
  - Worldwide operations and infrastructure

IronPort Architecture for Multi-Layered Email Security



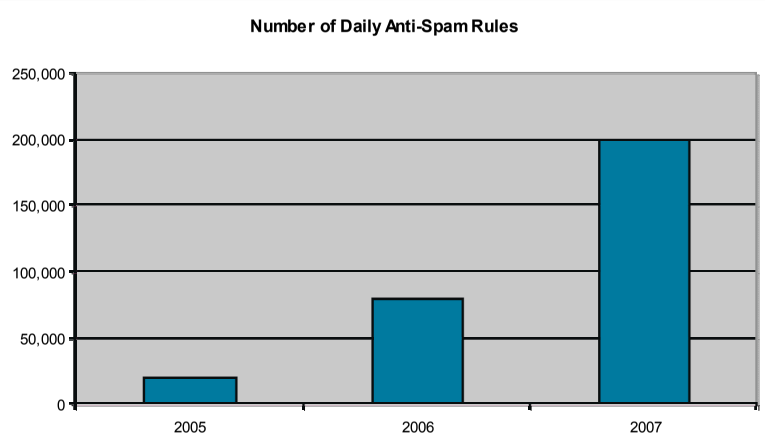
IRONPORT®

Spam Trends

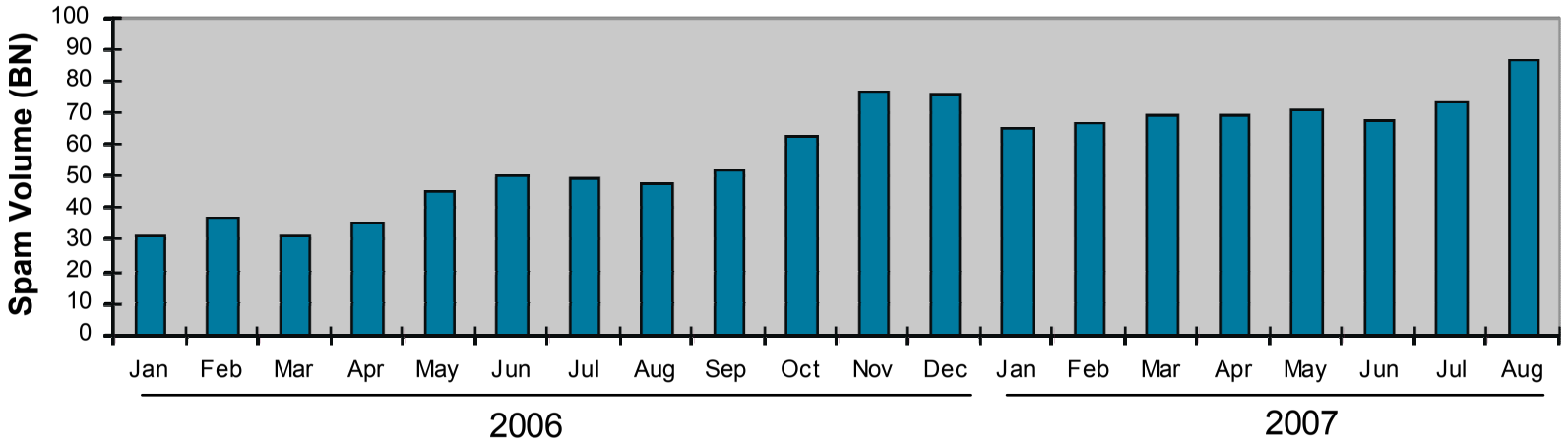
Through the first half of 2007

- *Spam volumes up 18% month over month*
- *New spammer tactics*
  - *-- Image link spam*
  - *-- PDF spam*
  - *-- XLS spam*

Increase In Average Daily Spam Rules



Average Daily Spam Volume By Month: 2006-2007



The IronPort SenderBase® Network

Global Reach Yields Benchmark Accuracy

The Dominant Force in Global Email and Web Traffic Monitoring…

- **30B+** queries daily
- **150+** Email and Web parameters
- **25%** of the World's Traffic

…Results in Accuracy and Advanced Protection

Spam Caught by Reputation

IronPort	**80%**
Secure Computing	50%
BorderWare	40%

Network Reach (Contributing Networks)

IronPort	**120,000**
Secure Computing	4,000
BorderWare	8,000

Virus Protection Lead

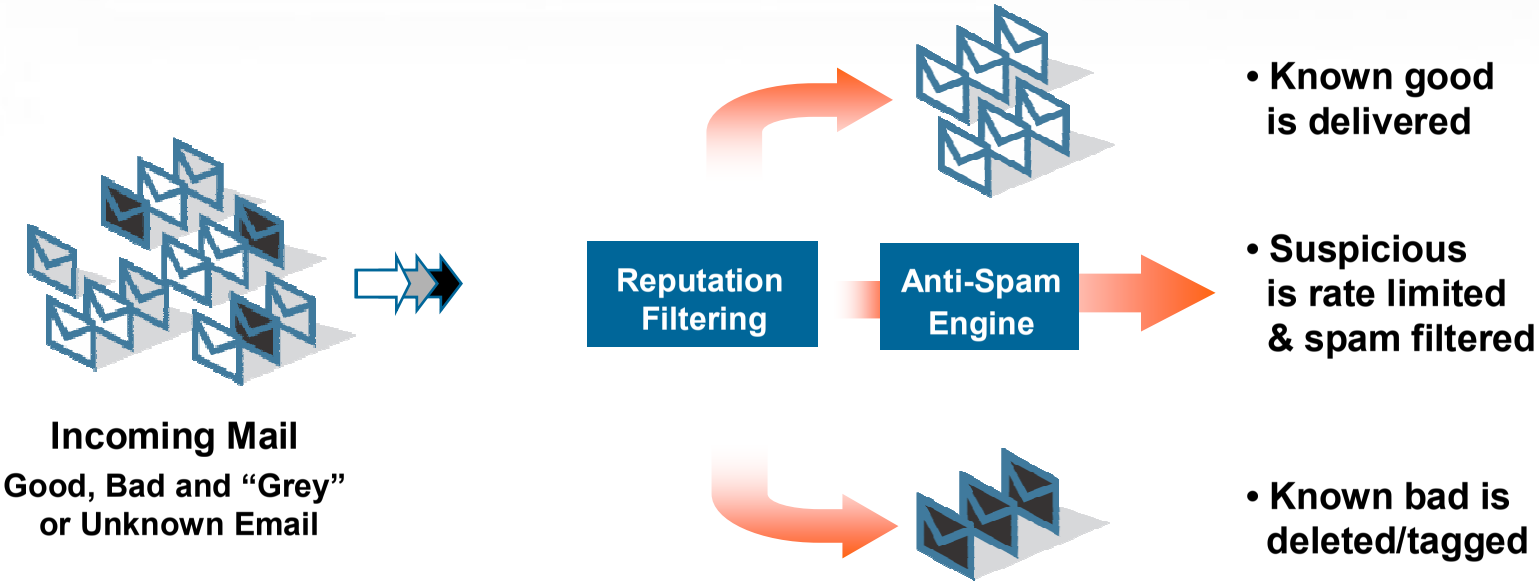
IronPort	**13 hours***
McAfee, Trend, Symantec, Sophos, CA, F-Secure	

** 6/2005 – 6/2006. 175 outbreaks identified. Calculated as publicly published signatures from the listed vendors.*

IRONPORT®

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

IronPort Reputation Filters™ Stop 80% of Hostile Mail at the Door….



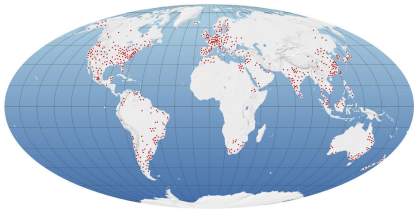
- IronPort uses identity & reputation to apply policy
- Sophisticated response to sophisticated threats

IRONPORT

IronPort Anti-Spam™

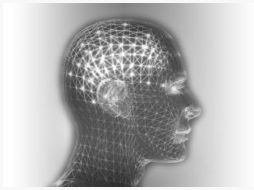
Backed By The Industry's Most Advanced Infrastructure

SenderBase



IronPort Threat Operations Center

SECURITY MODELING



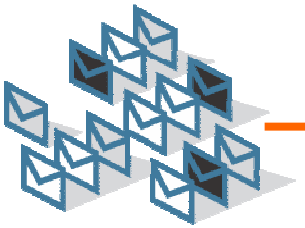
- *Machine Generated Rules*
- *Threat Evidence Clustering*

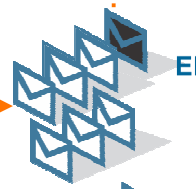
SECURITY ANALYSTS

- *Human Generated Rules*
- *24 x 7, 32 languages*

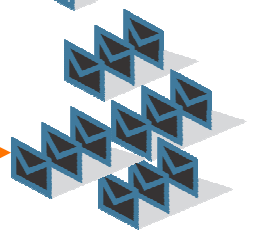
Over 100,000 updates daily

Context Adaptive Scanning Engine



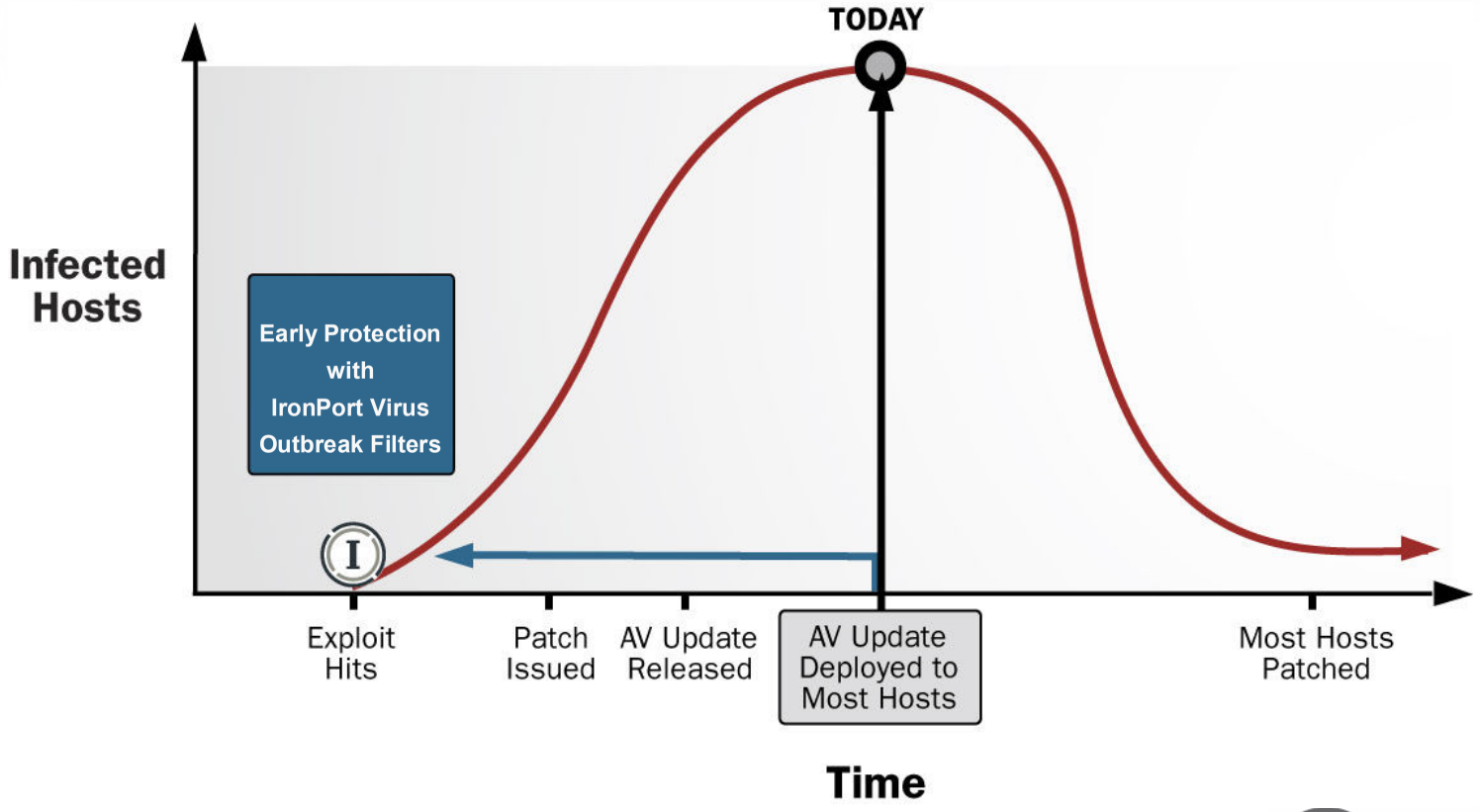


END-USERS



IronPort Virus Outbreak Filters™

First Line of Defense



IRONPORT®

IronPort Virus Outbreak Filters Advantage

Virus Name	Date	Virus Description	Lead Time (hh:mm)
Troj/Yar-A	5/24/07	Widely-spammed out email teaser promising a trailer of the film "Pirates of the Caribbean 3“. Downloads spyware onto infected computers.	3:20
Trojan.Dropper	5/10/07	Trojan that attempts to download malicious code.	10:40
W32.Virut!dr	4/12/07	Spammed email that asks recipients to open attachments entitled “document.txt.exe” and “video.zip”. Downloads spyware onto infected computers.	31:12
Troj/DwnLdr-GFN	3/4/07	Installs backdoor and communicates via HTTP, thus bypassing firewall filters.	17:31
W32/WowPWS-AU	3/3/07	Mass mailing worm that sends emails with the subject: "Chinese test missile obliterates satellite!“. Asks users to open attached file that, when opened, installs spyware.	6:51
Troj_Agent.JAW	1/14/07	Spammed email message that contains a seemingly benign PDF attachment. Once attachment is opened, backdoor is installed for remote hackers to access the PC.	20:08

Average lead time*……over 13 hours

Outbreaks blocked * ……175 outbreaks

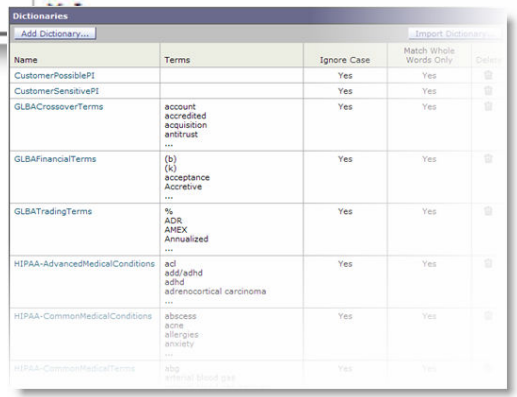
Total incremental protection*……over 94 days

**May 2006 – June 2007. Calculated as publicly published signatures from the following vendors: Sophos, McAfee , Trend Micro, Computer Associates, F-Secure, Symantec and McAfee. If signature time is not available, first publicly published alert time is used.*

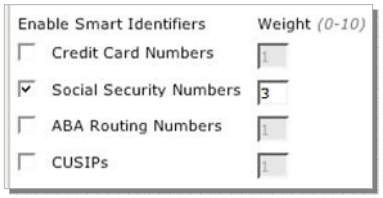
Data Loss Prevention:
Integrated Scanning and Remediation

Scanning Work Flow

Pre-Defined Filters

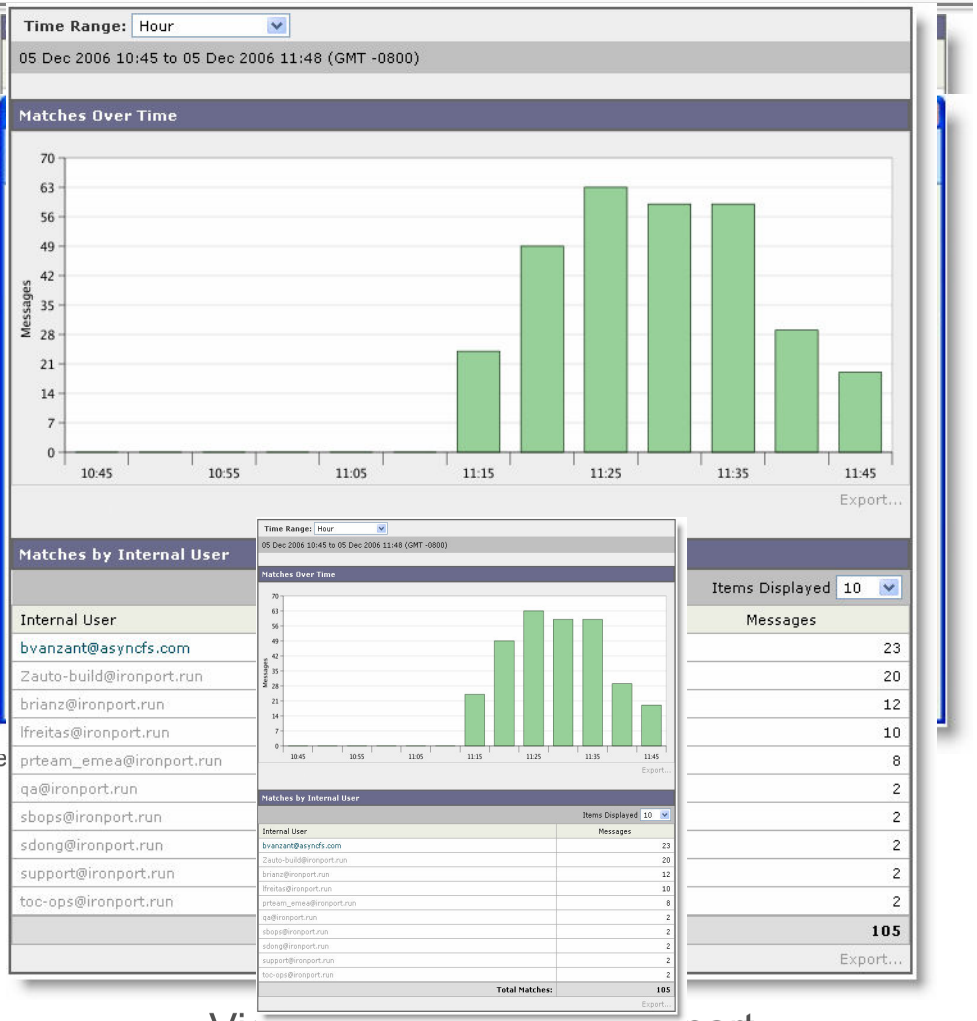


Compliance Dictionaries



Smart Identifiers

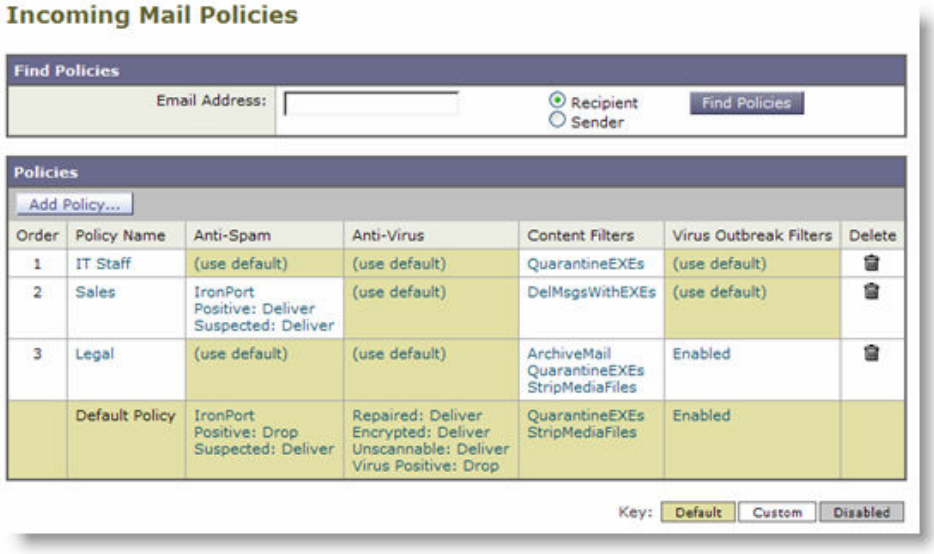
Remediation Work Flow



View HIPAA Violation Report

IronPort Email Security Manager™

Single view of policies for the entire organization



Categories: by Domain, Username, or LDAP

- Allow all media files
- Quarantine executables

IT

- Mark and Deliver Spam
- Delete Executables

SALES

- Archive all mail
- Virus Outbreak Filters disabled for .doc files

LEGAL

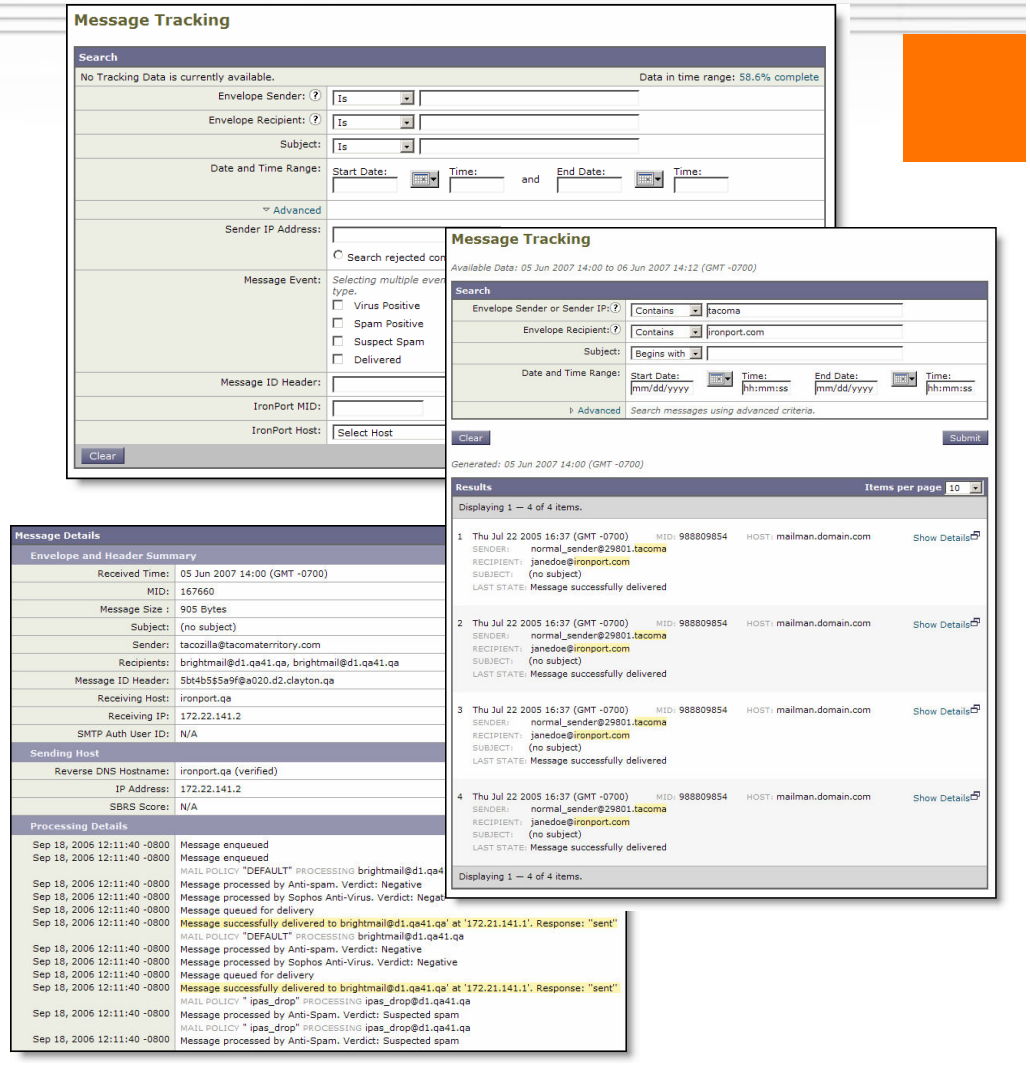
"Email Security Manager serves as a single, versatile dashboard to manage all the services on the appliance." *– PC Magazine, 2/22/05*

IRONPORT®

IronPort M-Series

Centralized Reporting and Message Tracking

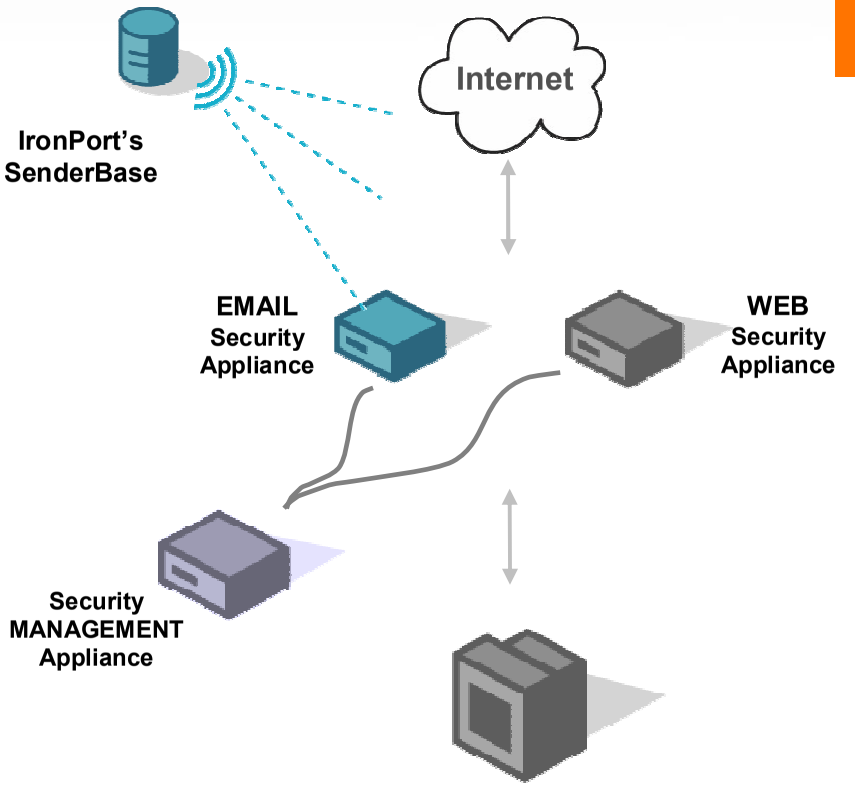
- Aggregated IronPort Email Security Monitor reports available on a central IronPort M-Series interface
- Helps administrators answer help desk calls quickly and easily
  - “Joe sent me an email, but I never received it.”
- Easier alternative to searching log files
  - Gives one place to search for messages across different appliances



Web Security Overview

IronPort®

IronPort® Perimeter Security Appliances



Web Security | Email Security | Security management

IRONPORT®

IronPort + Cisco

Extending Market Leadership

- **Customer Leadership**
  - Over 6,000 customers globally
  - 99% customer retention rate
- **Technology Leadership**
  - Industry leading email and Web security applications and management tools
- **Global Leadership**
  - Worldwide operations and infrastructure

Web Traffic: Clear & Present Risks

The Circle of Risk

Malware & Acceptable Use Policy (AUP) violations

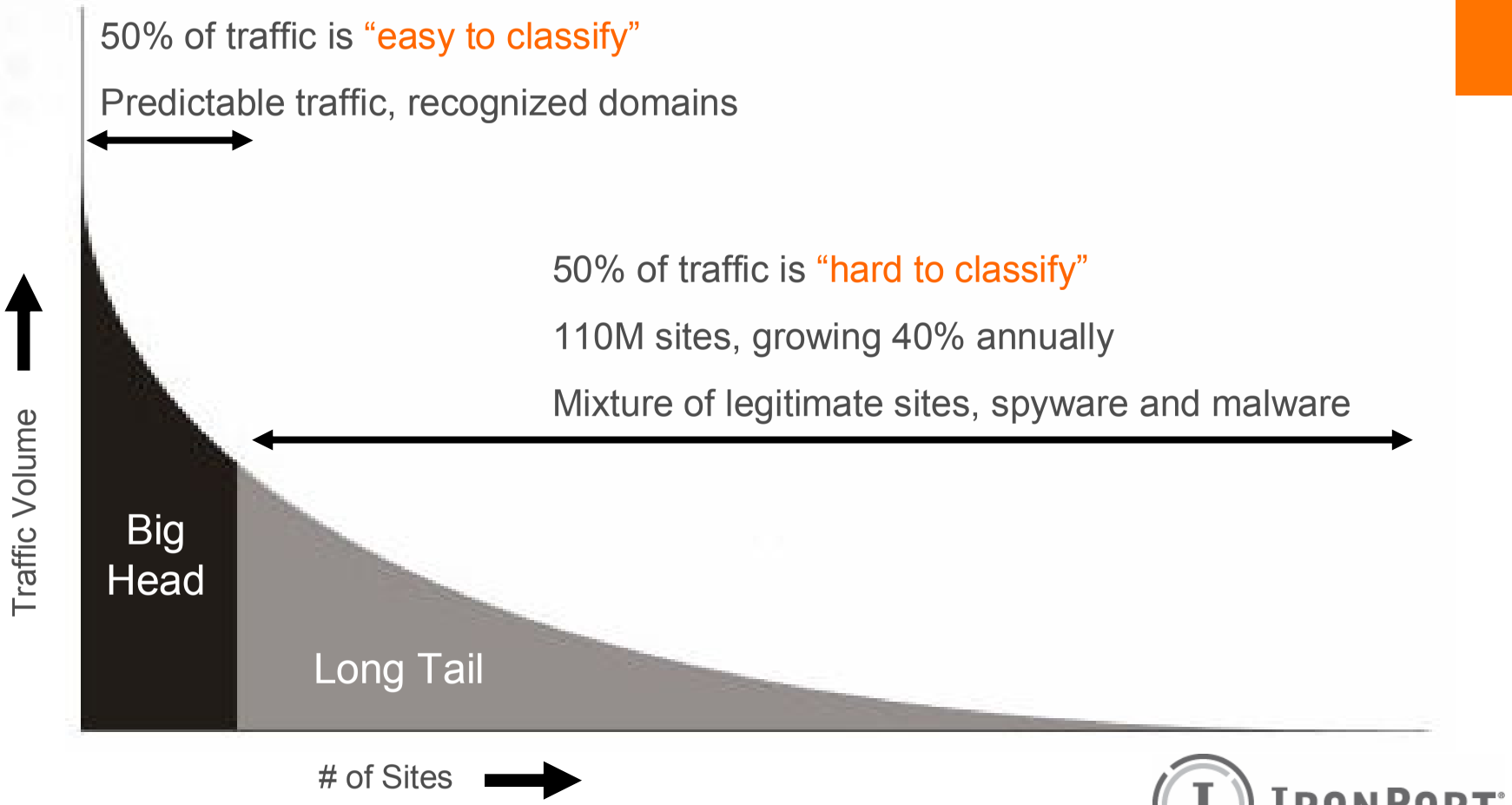
35-40% of Web usage is non-business related
(Source: IDC Research)

75%+ of enterprises are infected with spyware & malware
(Source: IDC Research)

IRONPORT

Web Traffic

The Long Tail Gets Longer



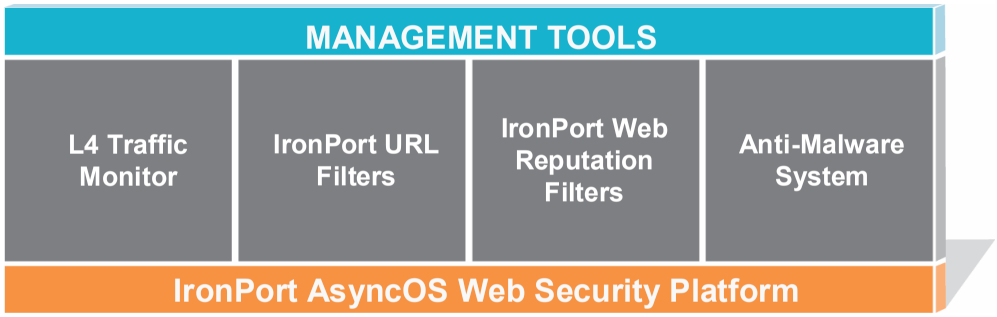
IRONPORT

IronPort S-Series™

Next Generation Web Security Platform

- Layer 4 (L4) traffic monitor inspects all traffic
- Web reputation for preventive filtering
- Integrated complete content inspection
- Acceptable Use URL filtering for corporate policy enforcement

IronPort S650/S350
Web Security System

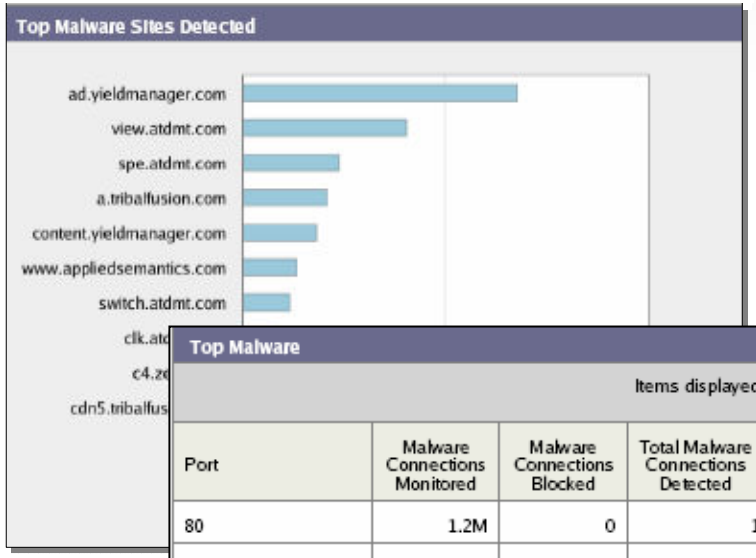


IRONPORT®

Detecting Existing Client Infections

Monitoring "Phone Home" Traffic

- Layer 4 Traffic Monitor
  - Scans all traffic, all ports, all protocols
  - Detects malware bypassing
  - Port 80
- 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 Reputation Filters™

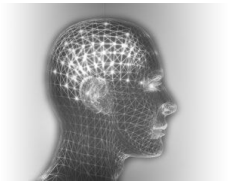
Data Makes the Difference

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…)
- Web Site History

THREAT PREVENTION IN REAL TIME

SenderBase Data



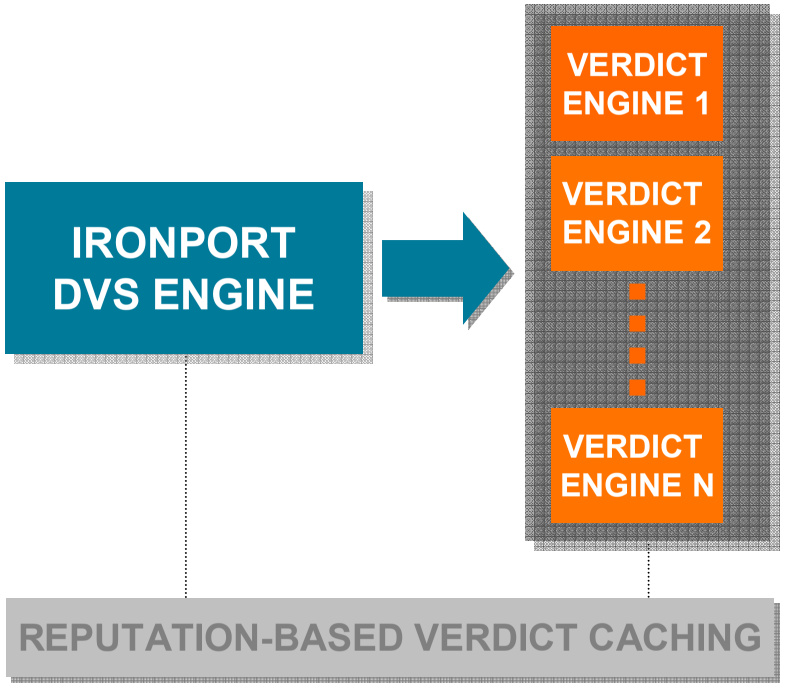
Data Analysis/ Security Modeling

Web Reputation Scores (WBRS) -10 to +10

IRONPORT®

IronPort Dynamic Vectoring and Streaming (DVS) Engine™

- High performance scanning
- Multiple verdict engine support
- Webroot
  - Large, accurate signature database
  - Automated threat research system (Phileas)
  - Backed by in-house Threat Research Team

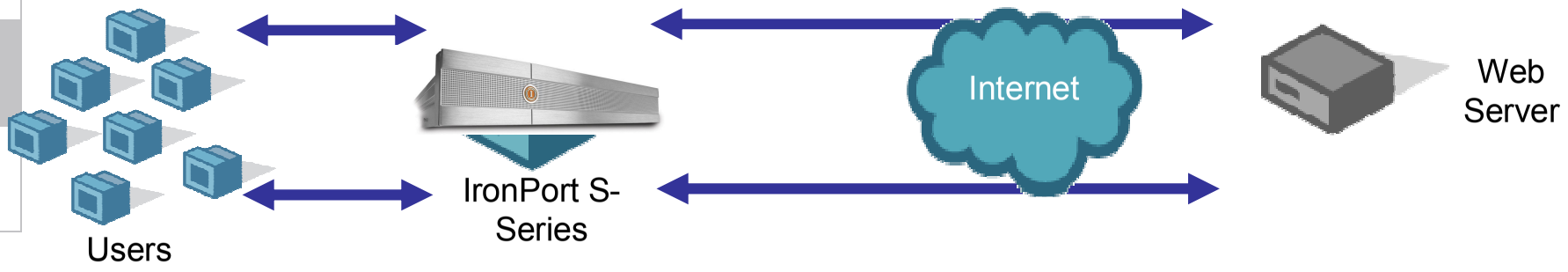


IRONPORT

HTTPS Scanning

Selective, Based on Trust

Decrypted • Inspected • Re-encrypted
Selectively on TRUST, Category, Source



Decrypted • Inspected • Re-encrypted
Selectively on Category, Source

IRONPORT

IronPort Web Security Monitor™

- System Overview
- Web Traffic Trends
- Site Activity
- Site Detail
- Client Activity
- Client Detail
- Category Detail
- Malware Details
- Malware Trends
- L4 Traffic Monitor
- Web Reputation

IronPort Perimeter Security Appliances

EMAIL & WEB OVERVIEW

IronPort is now part of Cisco.

CISCO

IRONPORT