IronPort Messaging Security

CISCO'S NEW STRATEGY AGAINST SPAM, VIRUSES AND SPYWARE

Mirko Schneider
Territory Manager Eastern Europe & Russia
IronPort - A CISCO Systems Business Unit

CISCO EXPO Croatia 2008

CISCO

IRONPORT™

The Power of SenderBase®

First, Biggest, Best Reputation System

Global Email and Web Traffic Monitoring

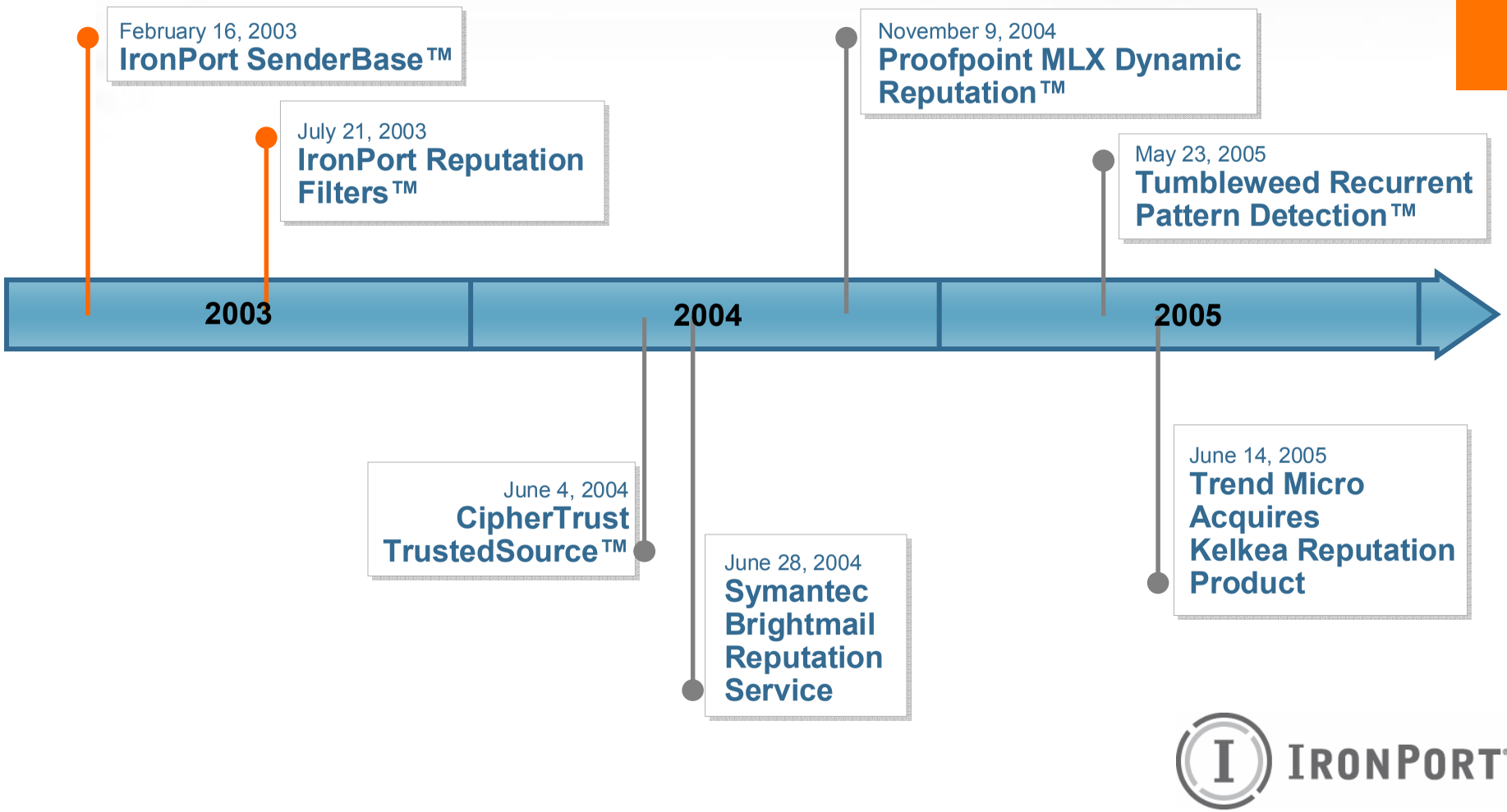
Over 100,000 contributing networks
Over 20M IP addresses tracked globally
View into **over 25%** of email traffic
Over 150 parameters tracked

cisco

IRONPORT®

Leading Edge Technology

Reputation Filtering Sets off Industry Scramble



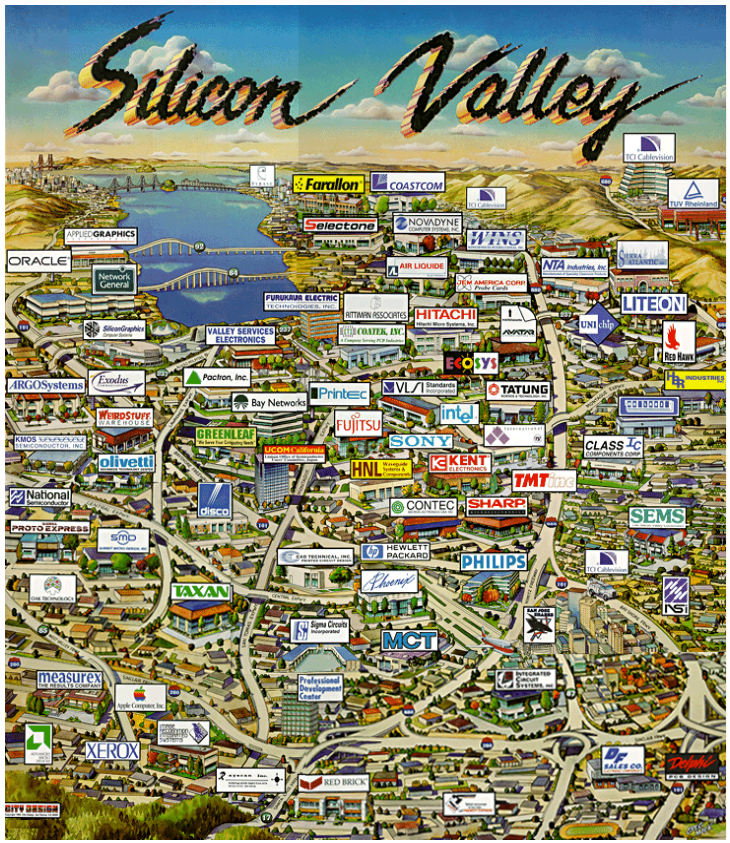
IRONPORT

Who is IronPort?

- Founded in 2000 by Email pioneers from Hotmail, ListBot, Yahoo
- idea: building the fastest and strongest gateway appliance
- HQ in California, Silicon Valley
- Worldwide 500+ employees

- Market growth rate = 50%
  IronPort growth rate = 100%
  revenue 2007: ~ 250m USD

- A Cisco Business Unit since mid 2007



CISCO

IRONPORT

IronPort – A CISCO Business Unit

- **Largest security acquistion**
- **5th largest acquisition ever**
- market consolidation:

Brigh
->

Cip
-> Secure

Postini
-> Google: 625m $

SurfControl
-> Websense: 400m $

CISCO

IRONPORT

The Principles of Industry Leadership

- Analyst Leadership
  - Gartner's Magic Quadrants 2006: Leader
  - IDC July 2007: market share leader
  - Radicati Market Quadrants 2007: Leader
- Customer Leadership
  - 52 of the World's Largest 100 Companies
  - 20+% of Global 2000
  - 12 of the 15 largest ISPs

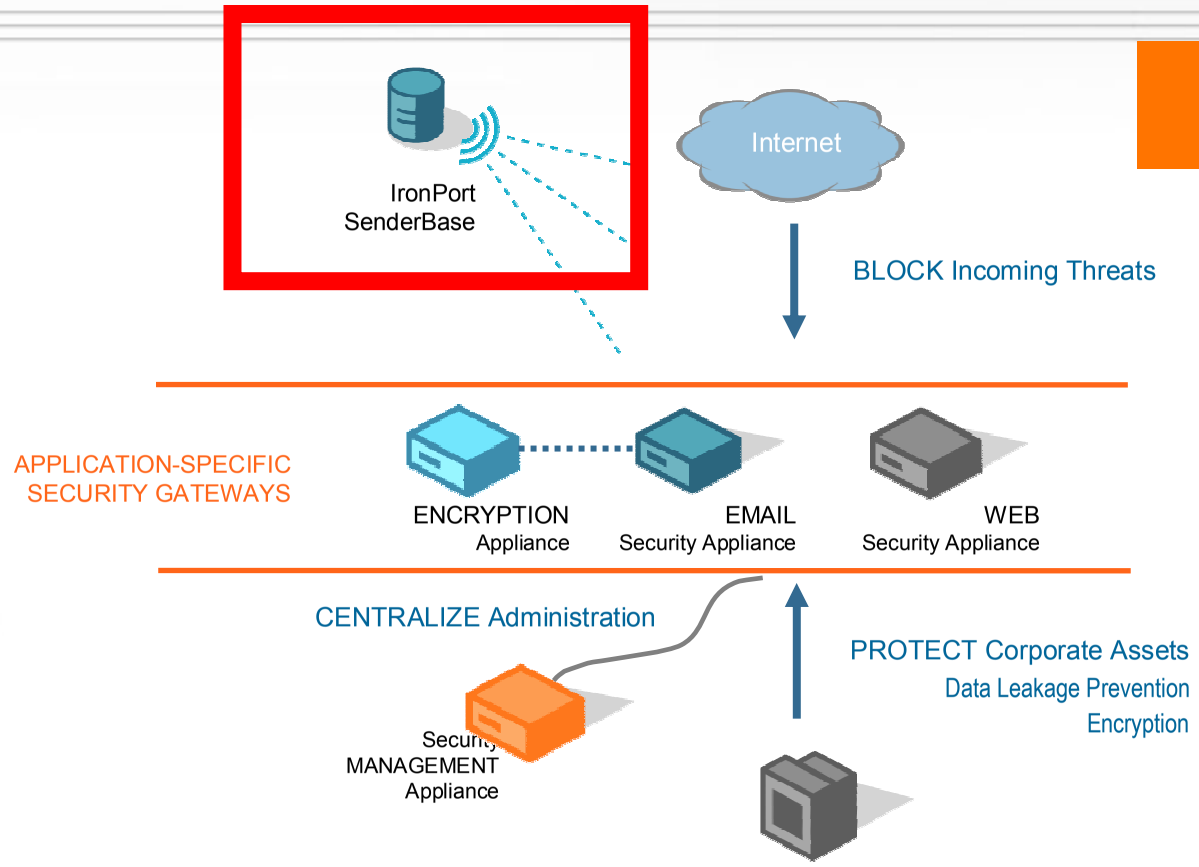
Success in Croatia

Raiffeisen BANK Austria d.d. Zagreb

CISCO

IRONPORT

IronPort® Gateway Security Products



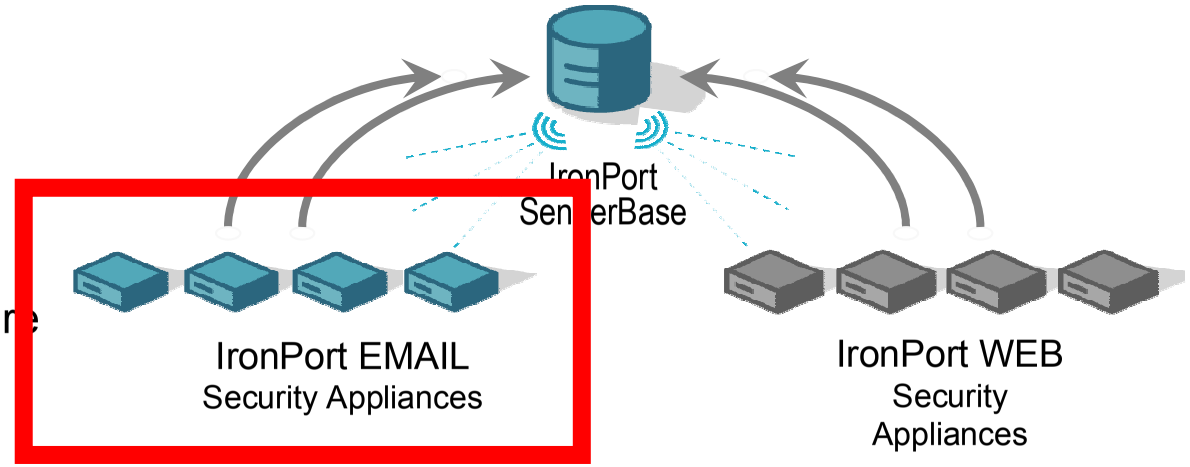
The IronPort SenderBase® Network

Global Reach Yields Benchmark Accuracy

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

- View into both email & Web traffic dramatically improves detection
- 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

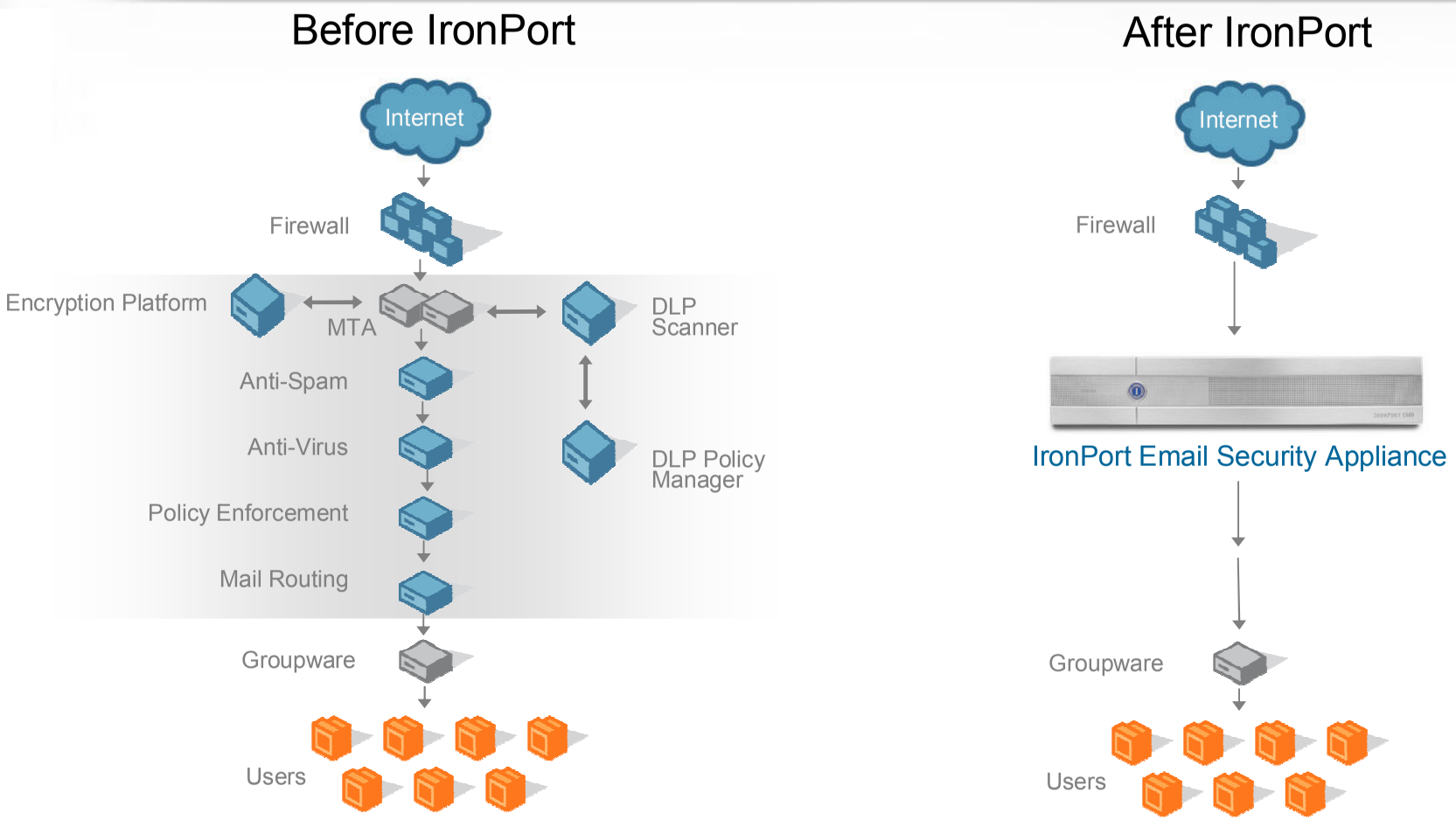


The Leader in Email Security

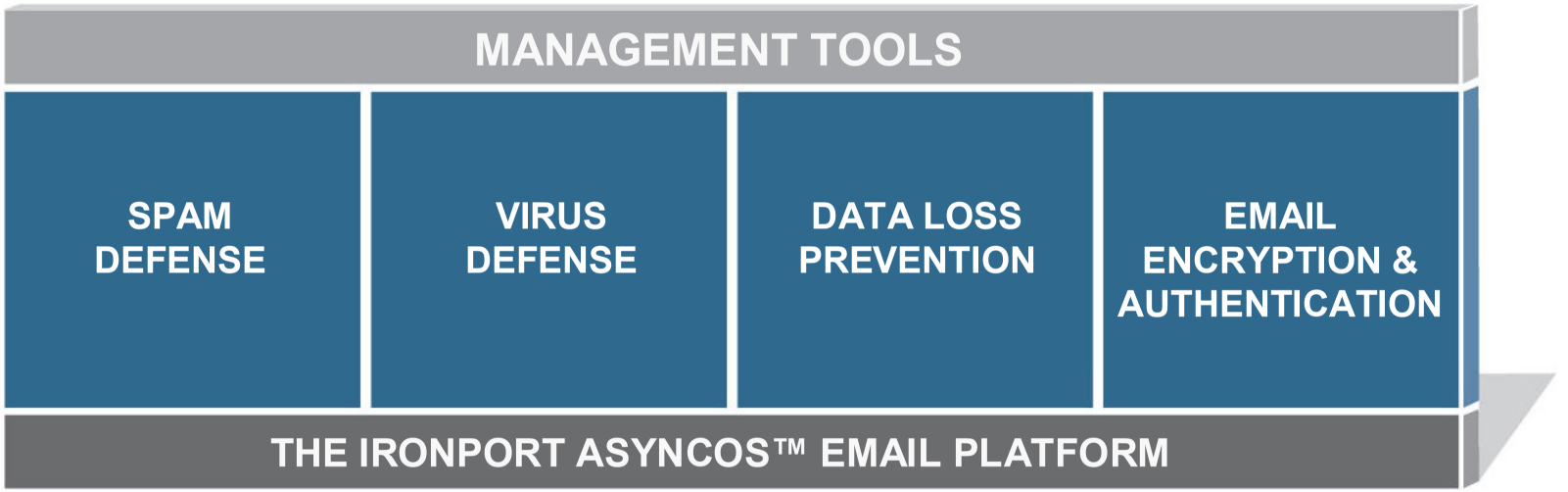
IronPort C-Series Appliance

IronPort Consolidates the Network Perimeter

For Security, Reliability and Lower Maintenance



IronPort Architecture for Multi-Layered Email Security

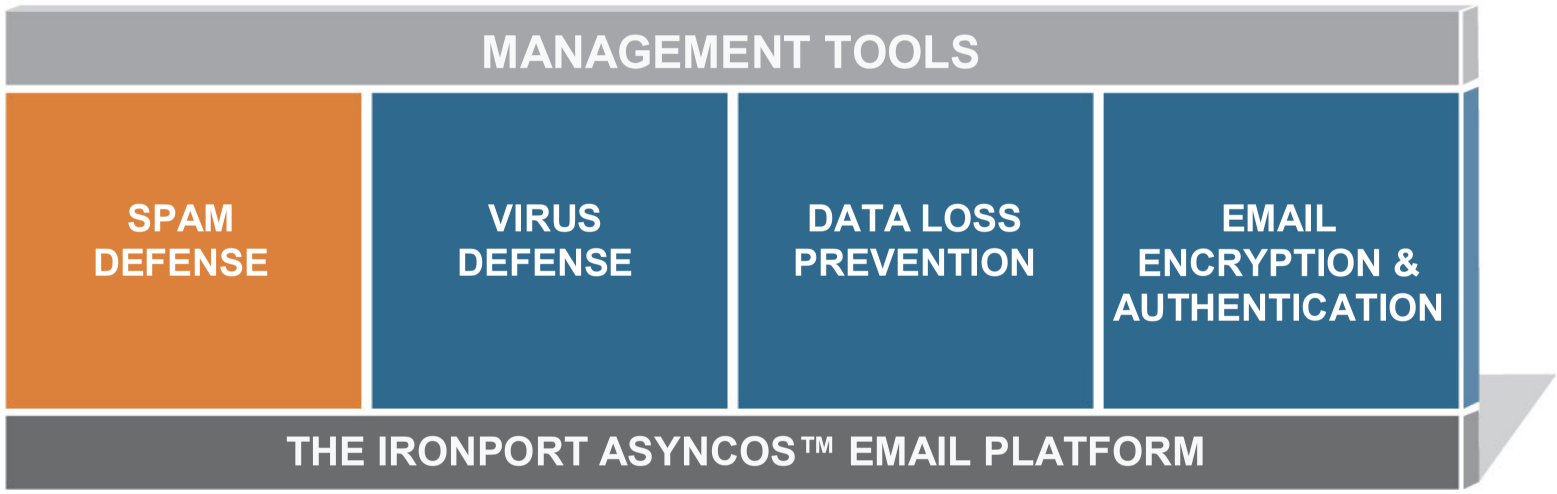


cisco

IRONPORT

Multi-layer Spam Defense

Best of Breed



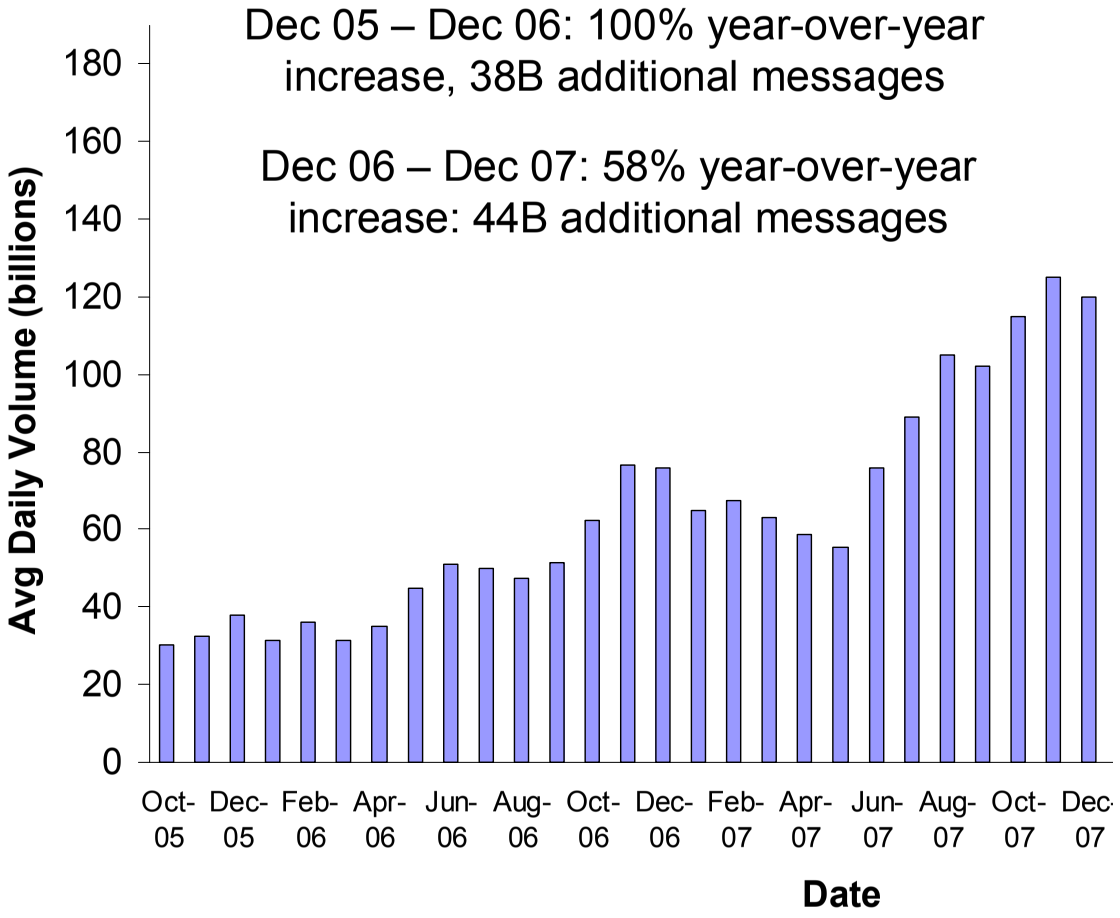
- **IronPort Reputation Filters** – the outer layer defense
- **IronPort Anti-Spam** - stops the broadest array of threats – spam, phishing, fraud

CISCO

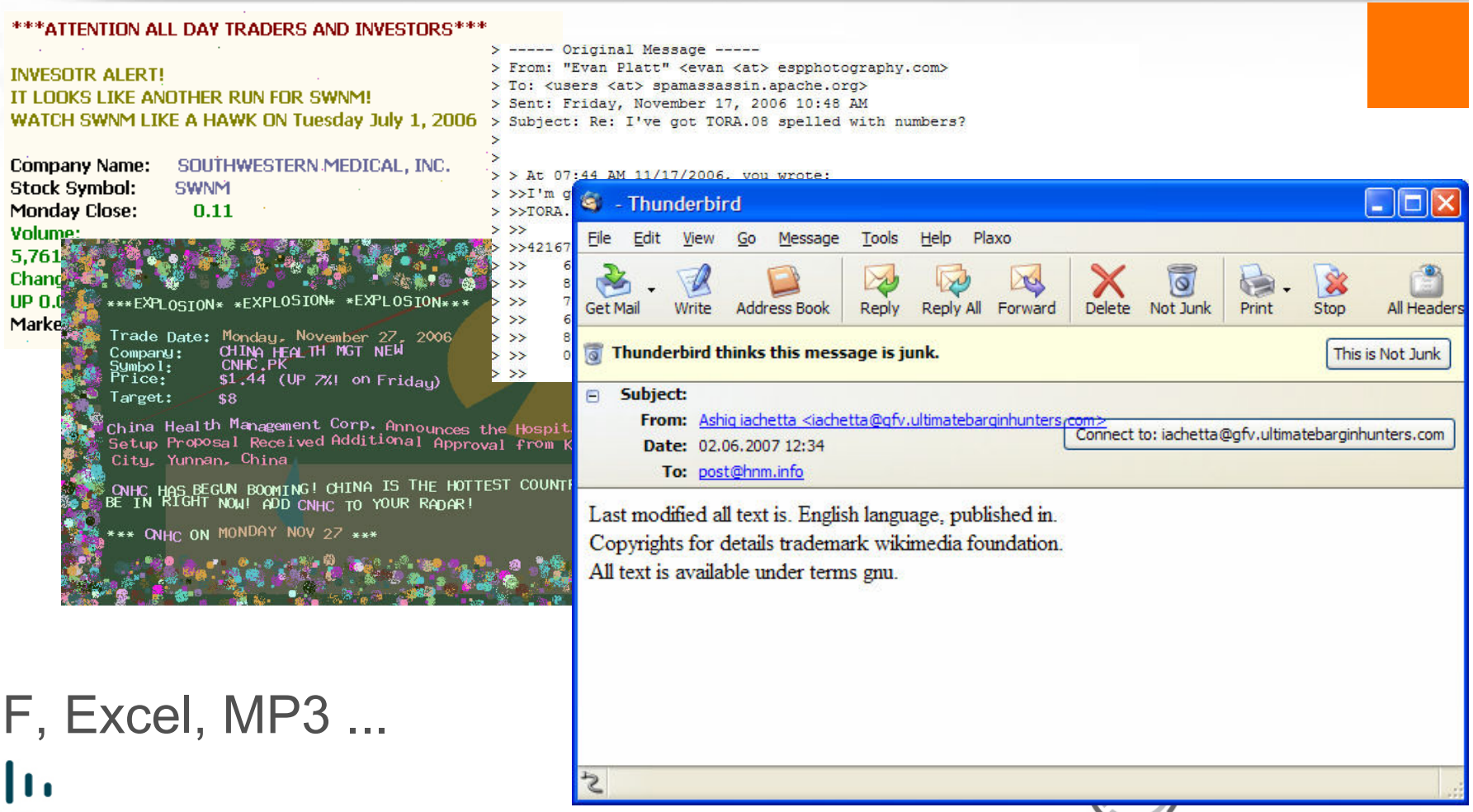
IRONPORT

Spam Volumes

2005 - 2008 Reality & Projections



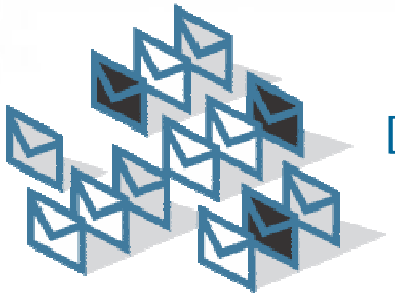
Spam is changing rapidly



PDF, Excel, MP3 ...

Multi-Layered Security

Preventive + Reactive = Defense in Depth



Preventive Layer

+

Reactive Layer

blocks ~ 80% of spam

Immediate Reaction to Threats	Adapts Over Time
Extremely High Performance	Computationally Intensive
Coarse Outer Layer	Fine-grained Inner Layer
Blocks or Rate Limits	Delete or Quarantine

cisco

IronPort SenderBase® Network

Global Reach Yields Benchmark Accuracy

The Dominant Force in Global Email and Web Traffic Monitoring…

- **5B+** queries daily
- **150+** Email and Web parameters
- **25%** of the World's Email Traffic

…Results in Accuracy and Advanced Protection

Spam Caught by Reputation

IronPort	**80%**
CipherTrust	50%
BorderWare	40%

Network Reach (Contributing Networks)

IronPort	**120,000**
CipherTrust	4,000
BorderWare	8,000

Virus Protection Lead

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

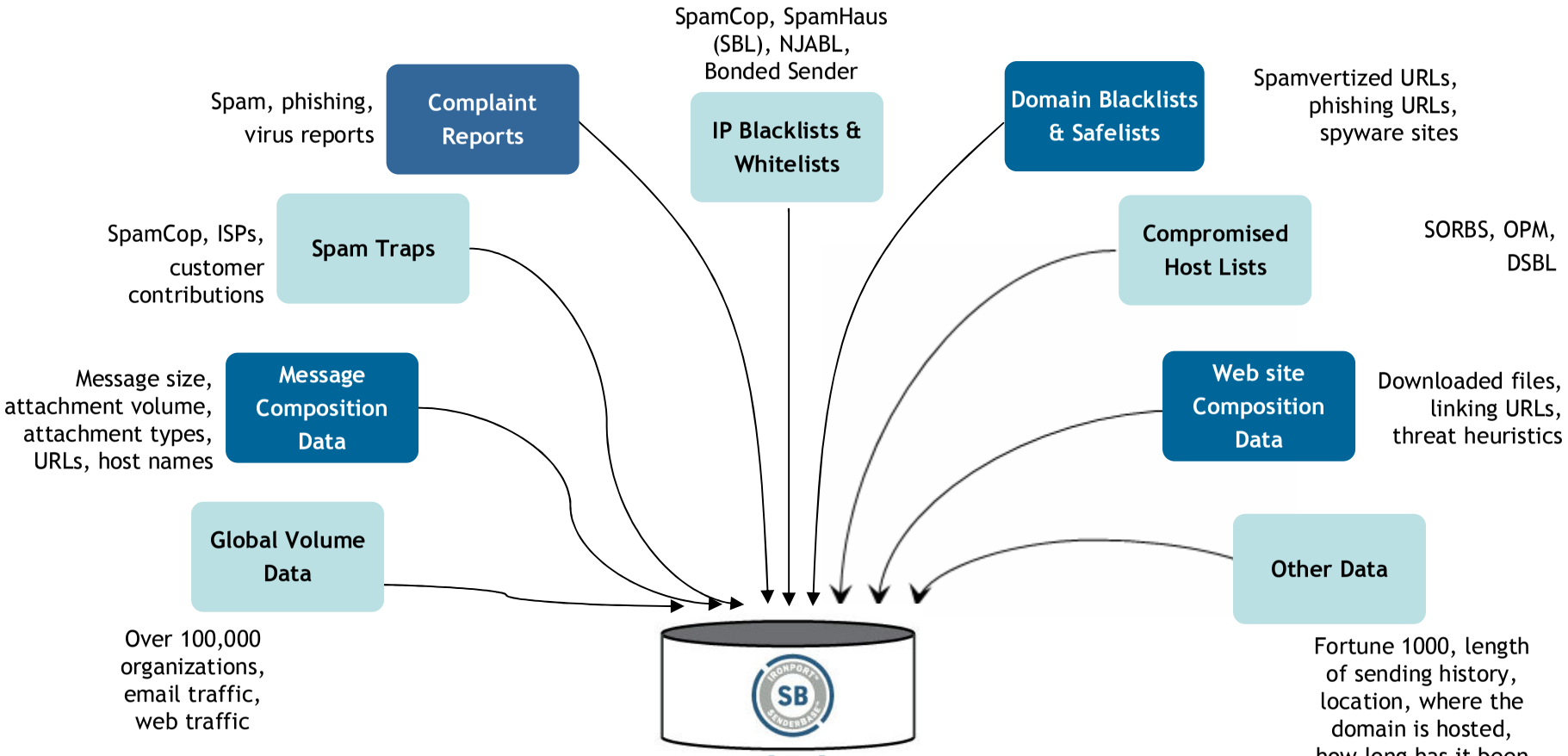
** 6/2005 – 6/2006. 175 outbreaks identified. Calculated as publicly published signatures from the listed vendors.*

IRONPORT®

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

IronPort SenderBase™ Reputation

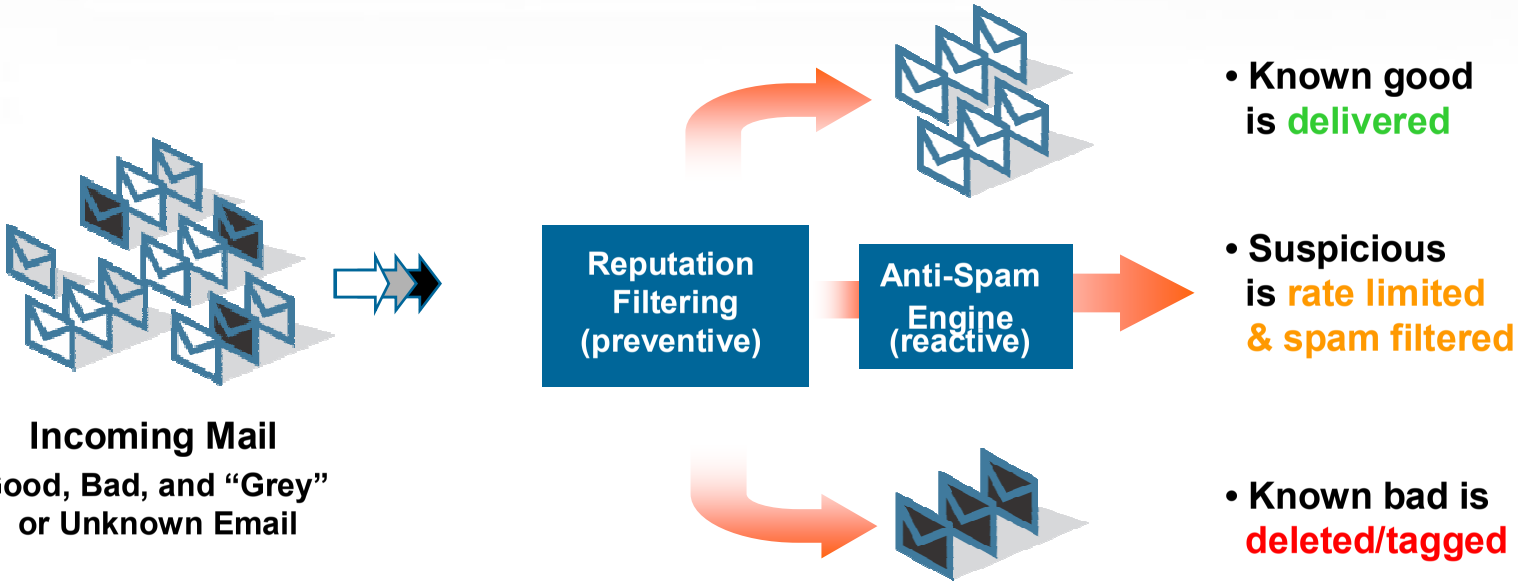
150 parameters for each IP



www.senderbase.org

Senderbase Reputation Score -10 to +10

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



- Reputation Filters is a switch point
- IronPort uses identity & reputation to apply policy
- Sophisticated response to sophisticated threats

CISCO

IRONPORT

IronPort Reputation Filters

Dell Case Study

- **Dell's challenge:**
  - Dell currently receives **26M** messages per day
  - Only **1.5M** are legitimate messages
  - **68 existing gateways** running Spam Assassin were not accurate
- **IronPort solution:**
  - Reputation Filters block over **19M** messages per day
  - **5.5M** messages per day scanned by anti-spam engine
  - Replaced **68** servers with **8** IronPort C60s

- Accuracy of spam filtering increased **10x**
- Servers consolidated by **70%**
- Operating costs reduced by **75%**

DELL™

"IronPort has increased the quality and reliability of our network operations, while reducing our costs."

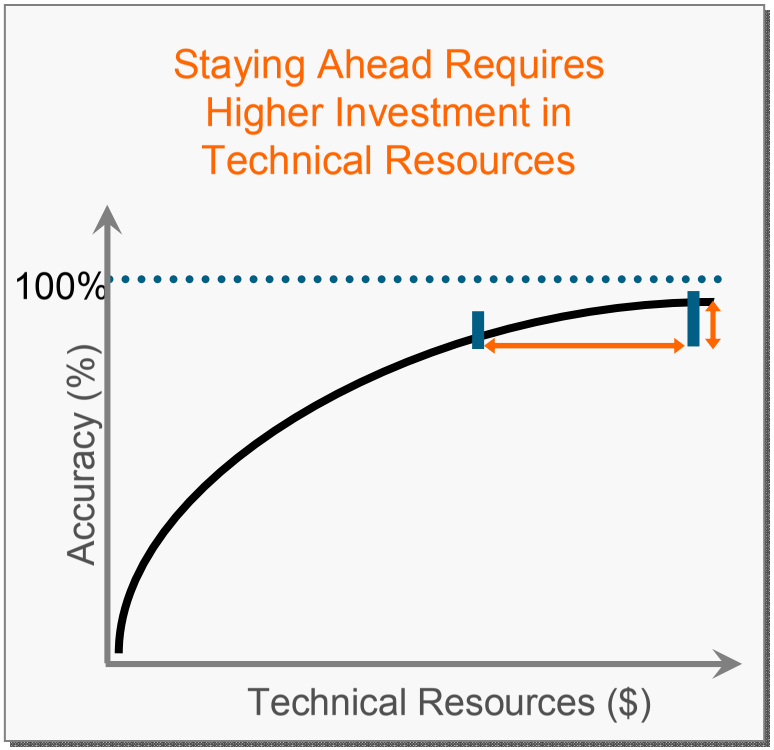
-- Tim Helmsetetter
Manager, Global Collaborative Systems Engineering and Service Management,

DELL CORPORATION

Self Defending Network 3.0

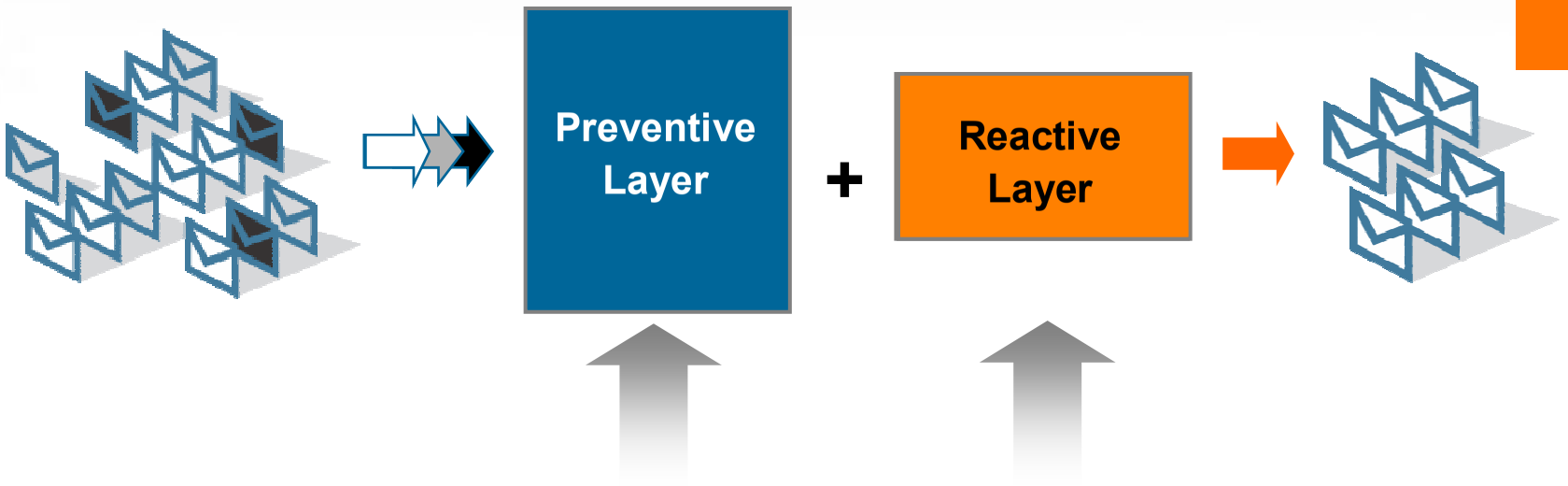
Extending Technology Leadership

- Wide Traffic Inspection
- Firewalls, routers, email appliances, web appliances, end point security agents
- sharing data across multiple protocols, across multiple network egress points, and across multiple networks world wide



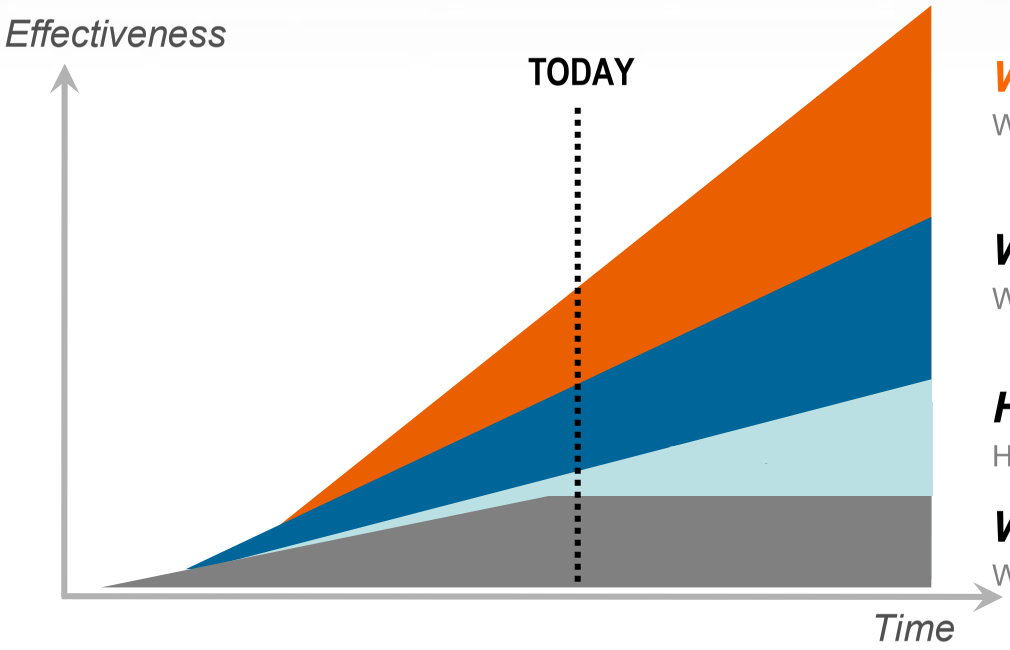
Multi-Layered Security

Preventive + Reactive = Defense in Depth



Immediate Reaction to Threats	Adapts Over Time
Extremely High Performance	Computationally Intensive
Coarse Outer Layer	Fine-grained Inner Layer
Blocks or Rate Limits	Delete or Quarantine

IronPort AntiSpam Broadens the Context with Web Reputation



Where? **Web Reputation**
Where does the call to action take you?

Who? **Email Reputation**
Who is sending you this message?

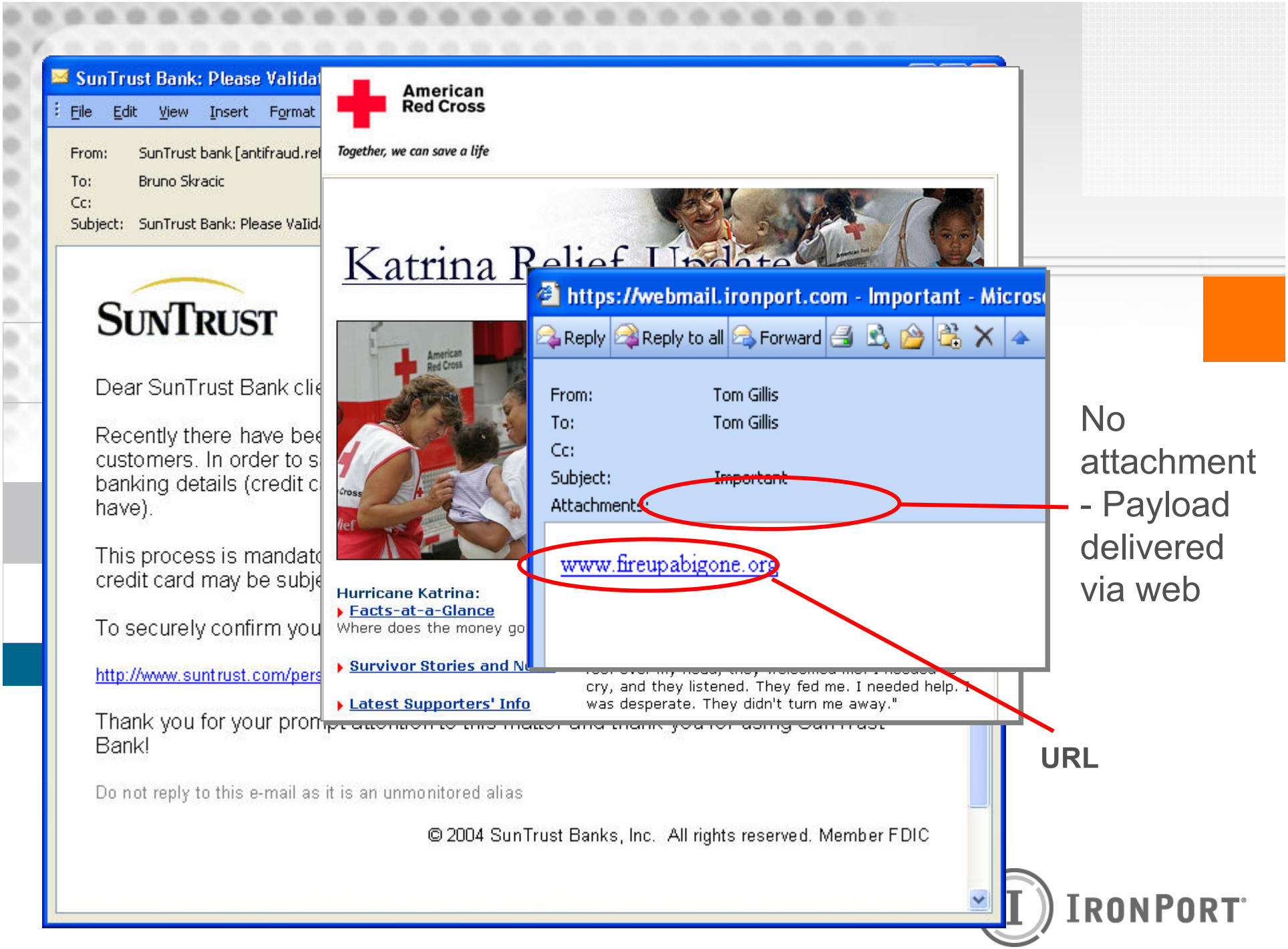
How? **Message Structure**
How was this message constructed?

What? **Message Content**
What content is included in this message?

- Content filtering techniques alone are inadequate
- Email reputation systems improved protection
- Combating new attacks demands Web reputation

CISCO

IRONPORT


SunTrust Bank: Please Validat
File Edit View Insert Format
From: SunTrust bank [antifraud.rel
To: Bruno Skracic
Cc:
Subject: SunTrust Bank: Please Valid
SUNTRUST
Dear SunTrust Bank clie
Recently there have bee
customers. In order to s
banking details (credit c
have).
This process is mandato
credit card may be subje
To securely confirm you
http://www.suntrust.com/pers
Thank you for your prom
Bank!
Do not reply to this e-mail as it is an unmonitored alias
© 2004 SunTrust Banks, Inc. All rights reserved. Member FDIC
American Red Cross
Together, we can save a life
Katrina Relief Update
Hurricane Katrina:
Facts-at-a-Glance
Where does the money go
Survivor Stories and N
Latest Supporters' Info
cry, and they listened. They fed me. I needed help. I
was desperate. They didn't turn me away."
https://webmail.ironport.com - Important - Micros
Reply Reply to all Forward
From: Tom Gillis
To: Tom Gillis
Cc:
Subject: Important
Attachments:
www.fireupabigone.org
No attachment - Payload delivered via web
URL
IRONPORT

IronPort SenderBase® Network

First, Biggest, Best Reputation System

Global Email and Web Traffic Monitoring

Over 100,000 contributing networks
Over 20M IP addresses tracked globally
View into **over 25%** of email traffic
Over 150 parameters tracked

CISCO

IRONPORT®

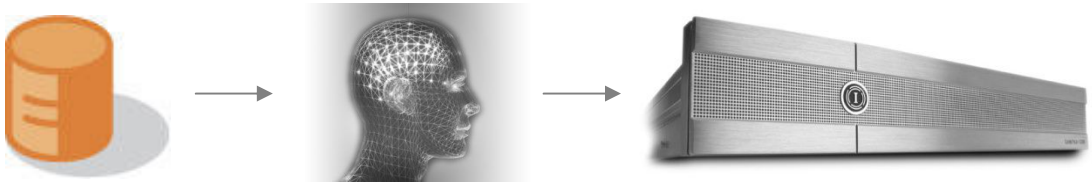
Web Reputation

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 REALTIME



SenderBase Data

Data Analysis/ Security Modeling

Web Reputation Scores (WBRS) -10 to +10

CISCO

IRONPORT

IronPort Anti-Spam

Press Reviews

InfoWorld

2007 Technology of the Year: Best Anti-Spam

Jan 2007

Competitors tested:
Symantec, Microsoft, Mirapoint, ProofPoint

"easy setup"

"excellent spam filtering"

"no tuning necessary"

"the fewest false positives of any solution tested"

infosecurity

Anti-Spam Bake-Off Winner

Dec 2006

Competitors tested:
CipherTrust, Borderware, Sophos, SonicWall

"The superiority of IronPort . . . seems abundantly clear"

"We did not have to rescue a single legitimate message"

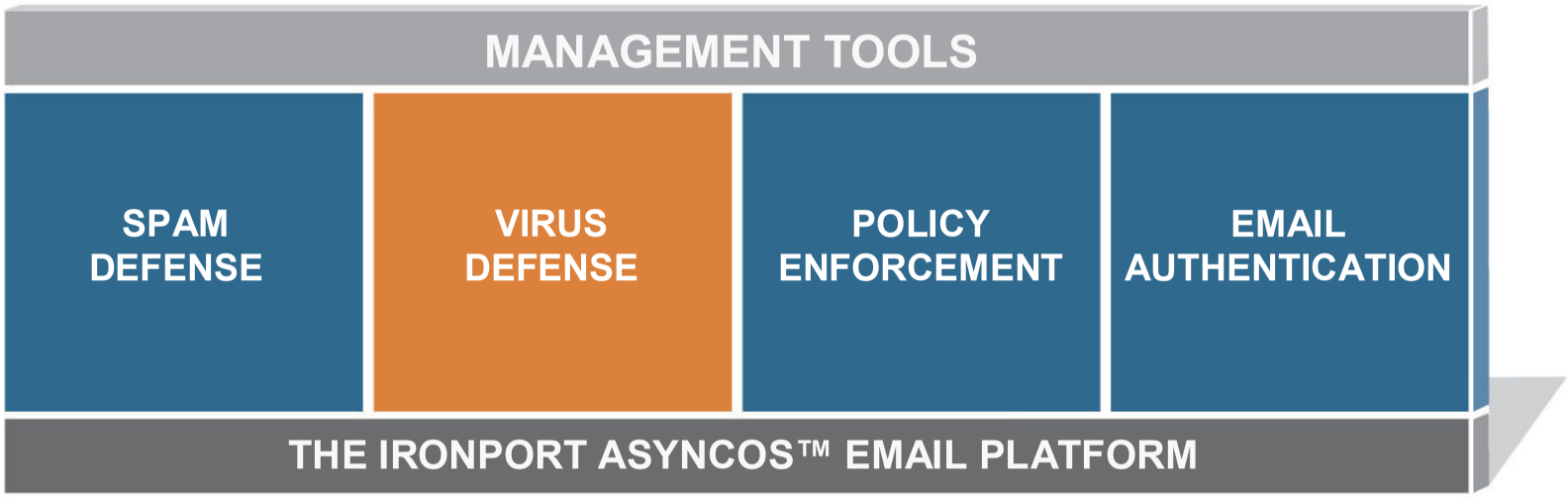
"(IronPort) is the absolute must from this test"

CISCO

IRONPORT

Multi-layer Virus Defense

Best of Breed



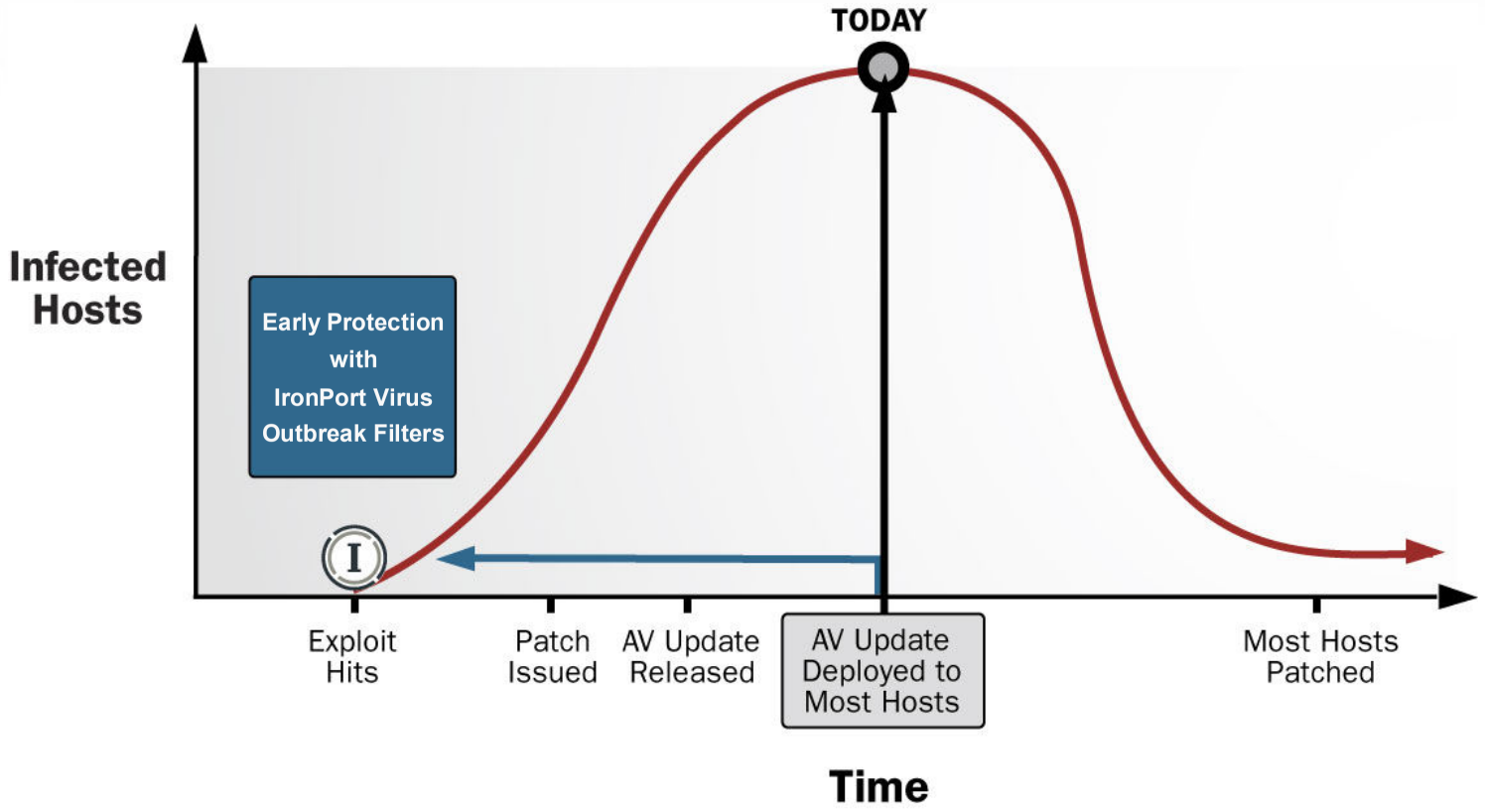
- **IronPort Virus Outbreak Filters** stop outbreaks 13 hours ahead of signatures
- **Sophos Anti-Virus** signature based solution with industry leading accuracy

CISCO

IRONPORT

IronPort Virus Outbreak Filters™

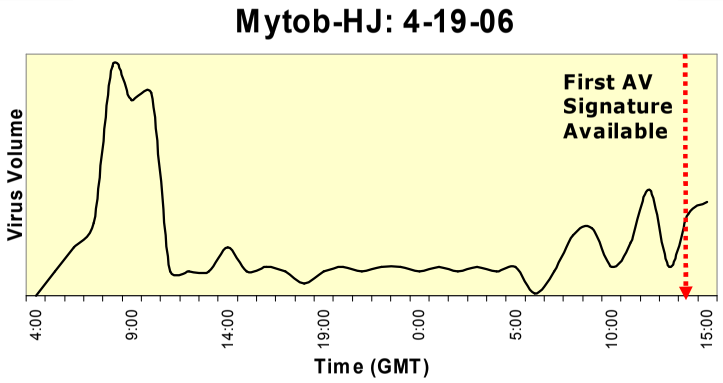
First Line of Defense

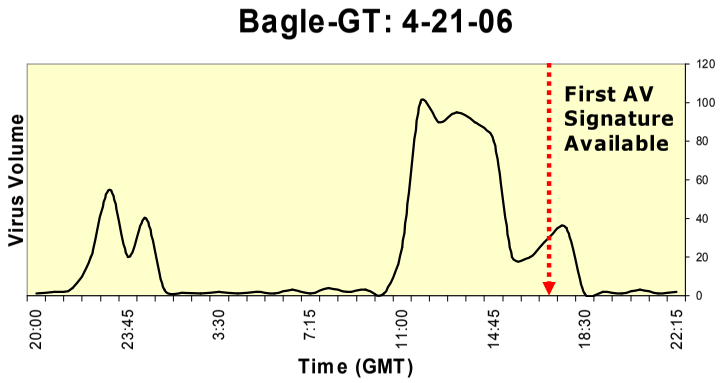


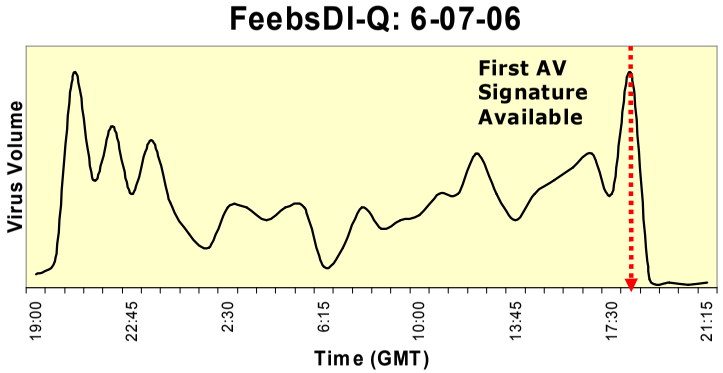
CISCO

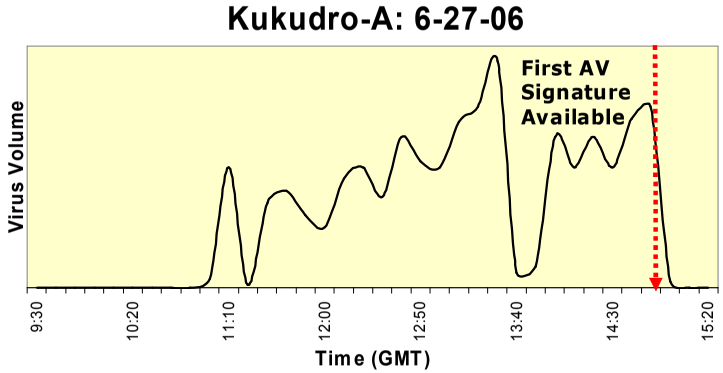
IRONPORT

Traditional AV Solutions Aren't Responding Quickly Enough . . .









TRONPORT

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

IronPort SenderBase® Network

First, Biggest, Best Reputation System

Global Email and Web Traffic Monitoring

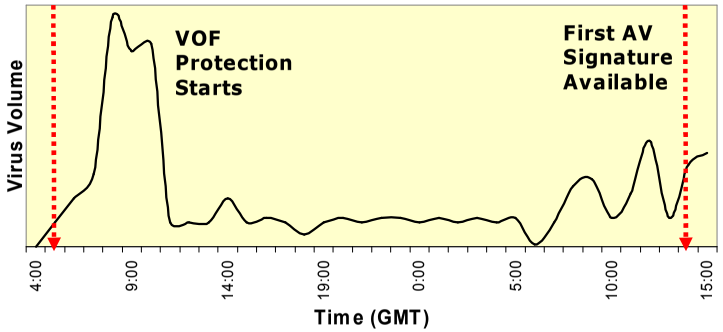
Over 100,000 contributing networks
Over 20M IP addresses tracked globally
View into **over 25%** of email traffic
Over 150 parameters tracked

CISCO

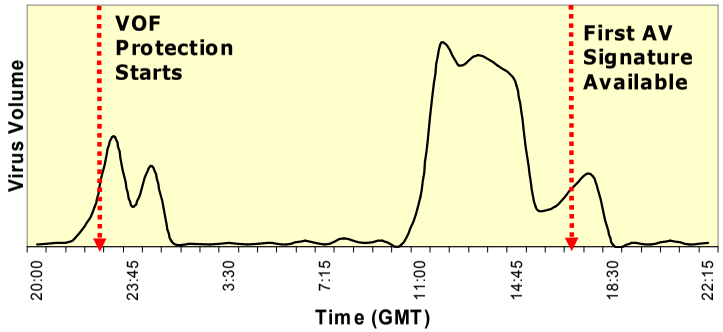
IRONPORT®

Introducing Virus Outbreak Filters

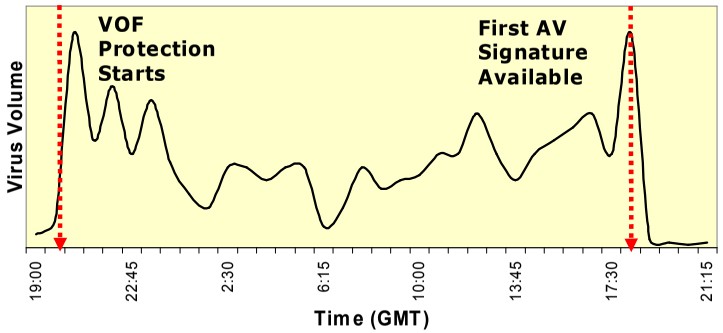
Mytob-HJ: ***32 hrs 57 mins Lead Time!***



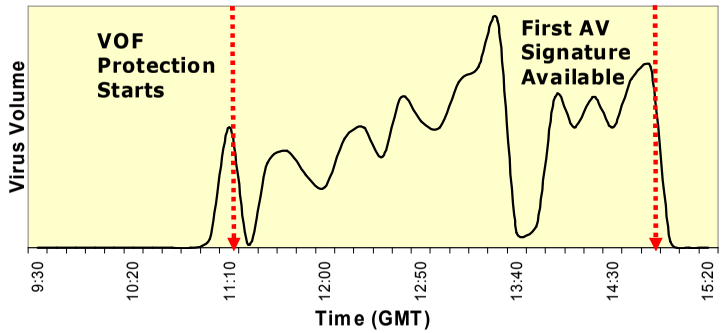
Bagle-GT: ***18 hrs 28 mins Lead Time!***



FeebsDl-Q: ***21 hrs 59 mins Lead Time!***



Kukudro-A: ***3 hrs 38 mins Lead Time!***



TRANPORT

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

Virus Outbreak Filters Advantage

Virus Name	Date	Virus Description	Lead Time (hh:mm)
Troj/Dloadr-BCK	7/24/07	Installs spyware on infected PCs.	10:06
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 spyware attachments entitled "document.txt.exe" and "video.zip".	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 spyware infected file.	6:51
Troj_Agent.JAW	1/14/07	Spammed email message that contains PDF attachment. Once attachment is opened, backdoor is installed for remote hackers to access the PC.	20:08

Average lead time*.....over 13 hours

Major Outbreaks blocked * .....175 outbreaks

Total incremental protection*.....over 94 days

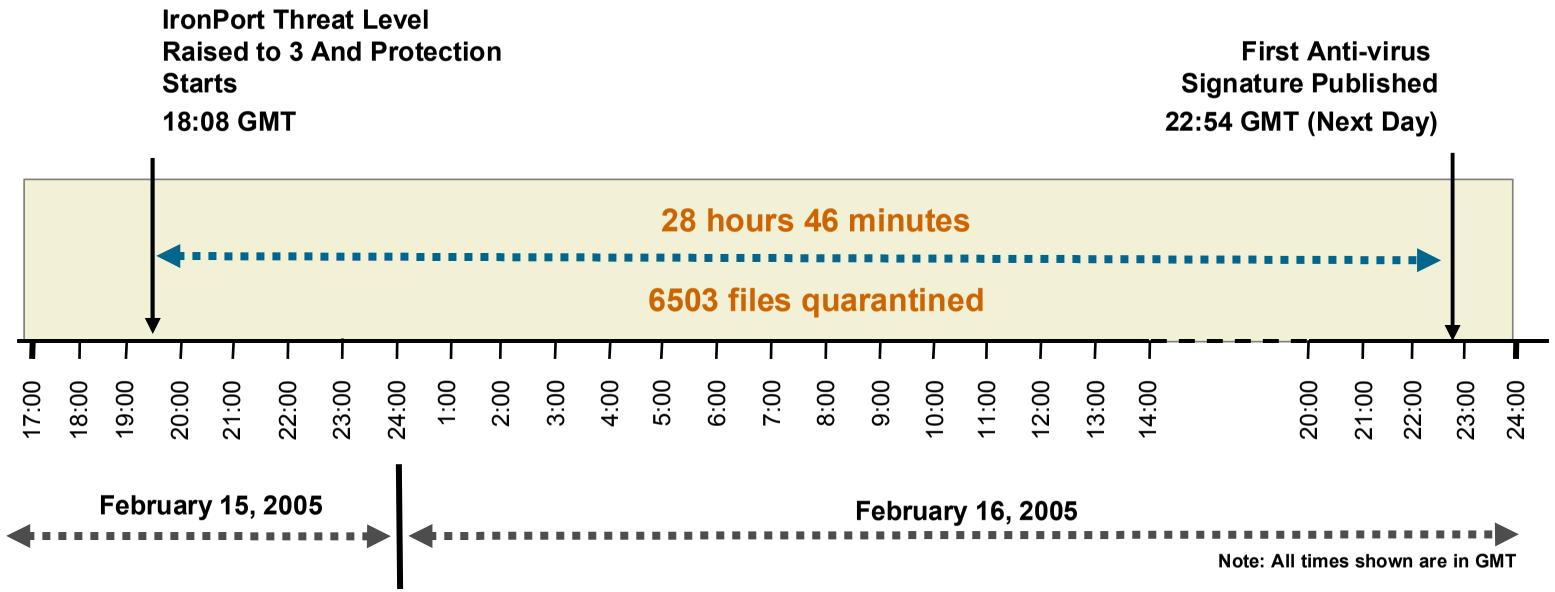
IRONPORT

** June 2005 –July 2006. 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.*

IronPort Outbreak Filters Protect
G2000 Company From MyDoom.BB

MyDoom Variant—MyDoom.BB (February 15, 2005)

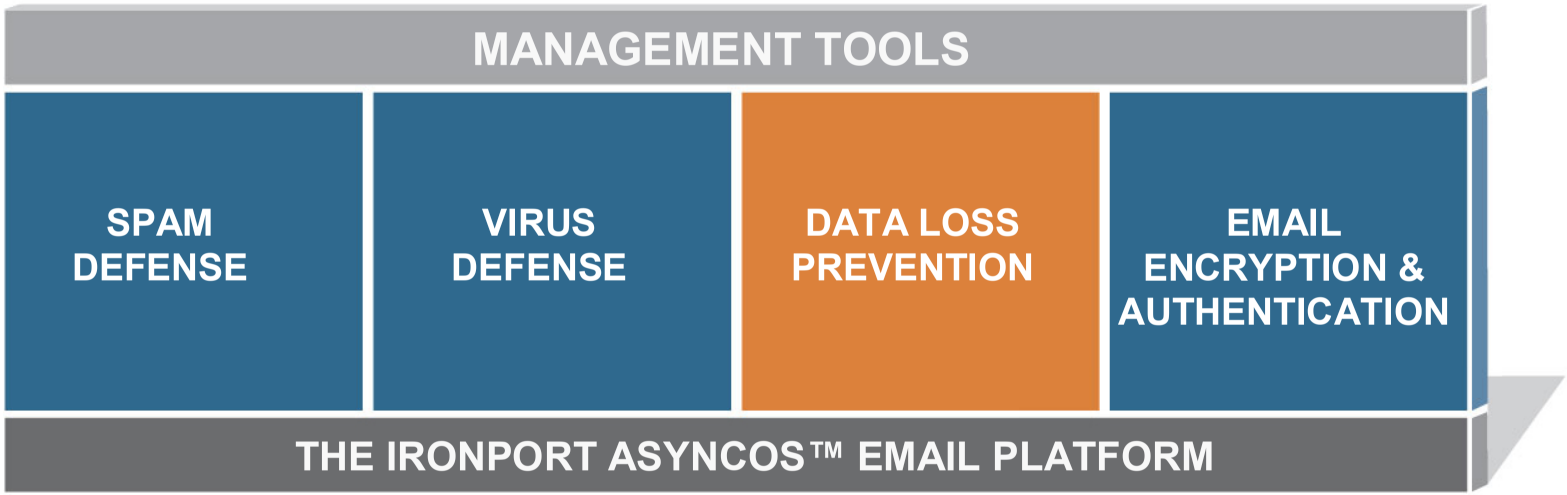
G2000 Company Protected By IronPort's Virus Outbreak Filters



$65K saved @ $200/desktop, 5% infected

IronPort Policy Enforcement

Inbound/Outbound Content Filtering for Compliance



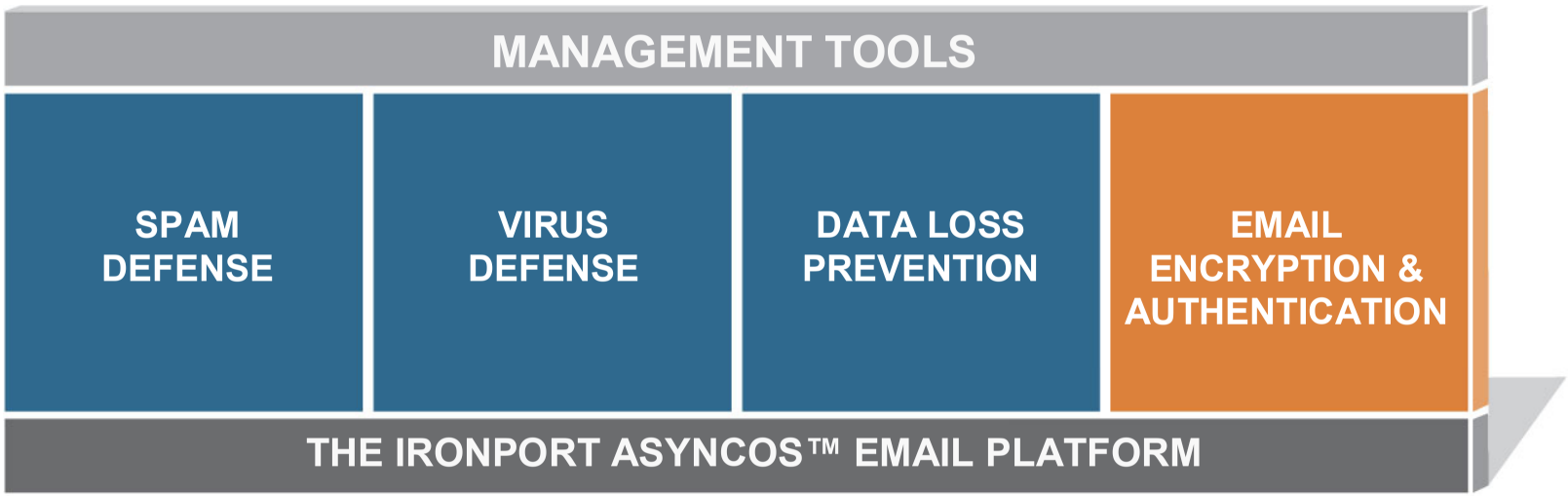
- **Flexible Policy Engine** from Blocking Attachments to Enforcing Regulatory Compliance
- **Compliance Solutions and Encryption** keep communications private and secure

cisco

IRONPORT

Email Encryption & Authentication

Superior Security and Identity Protection

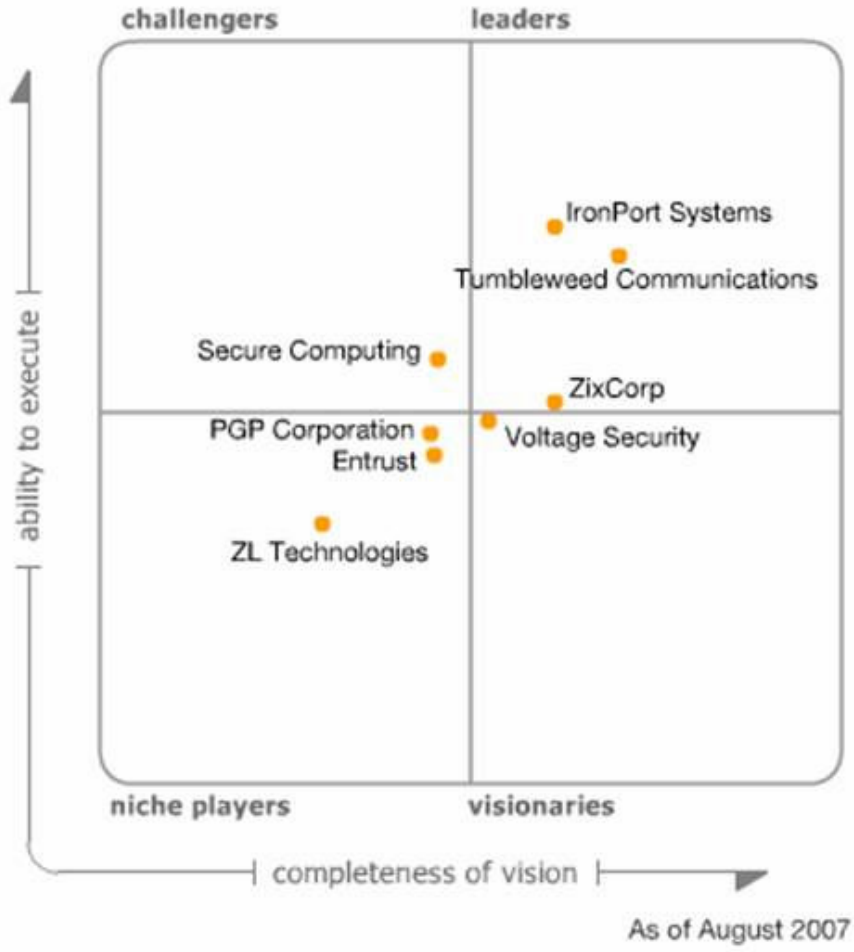


- **DomainKey Signing** - establishes and protects your identity on the Internet
- **IronPort Bounce Verification** – protects from misdirected bounce attacks
- **Directory Harvest Attack Prevention** –blocks attempts to steal email directory information

CISCO

IRONPORT

Leader in Email Encryption!



Gartner

Magic Quadrant for E-Mail Encryption Boundary 2007

Source: Gartner RAS Core Research

You need that competitive analysis?

Mail me at mschneider@ironport.com!

cisco

IRONPORT

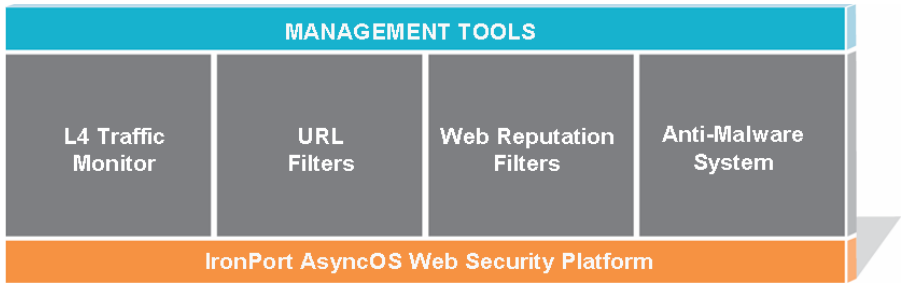
The Challenger in Web Security

IronPort S-Series Appliance

IronPort S-Series

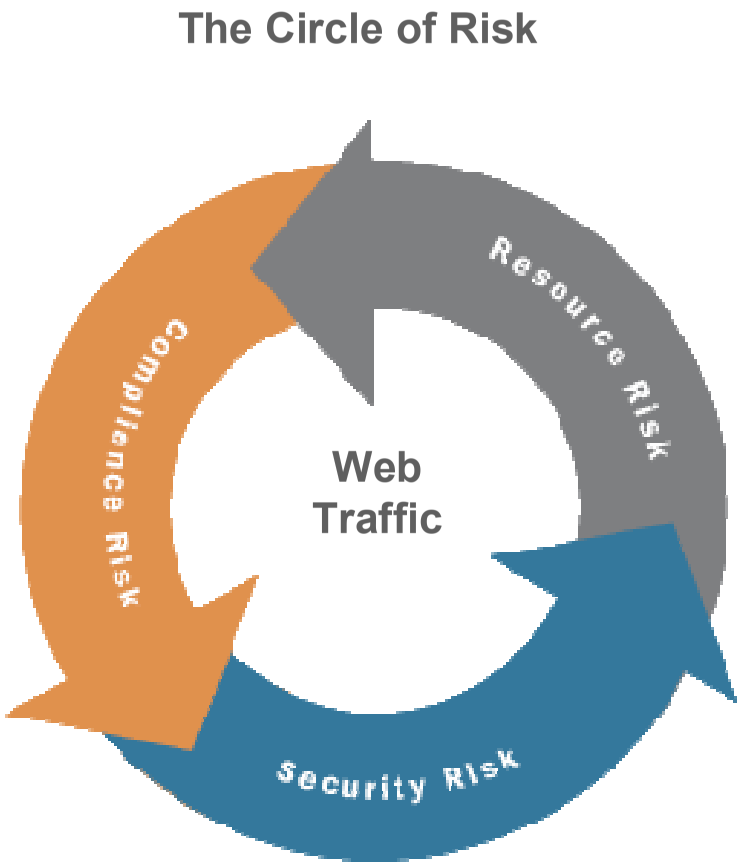
- Control & **secure** Web traffic
- Comprehensive management & visibility
- Industry-leading accuracy against Web-based threats
- Carrier-class performance

IronPort Web Security Appliance



Next Generation Web Security Platform

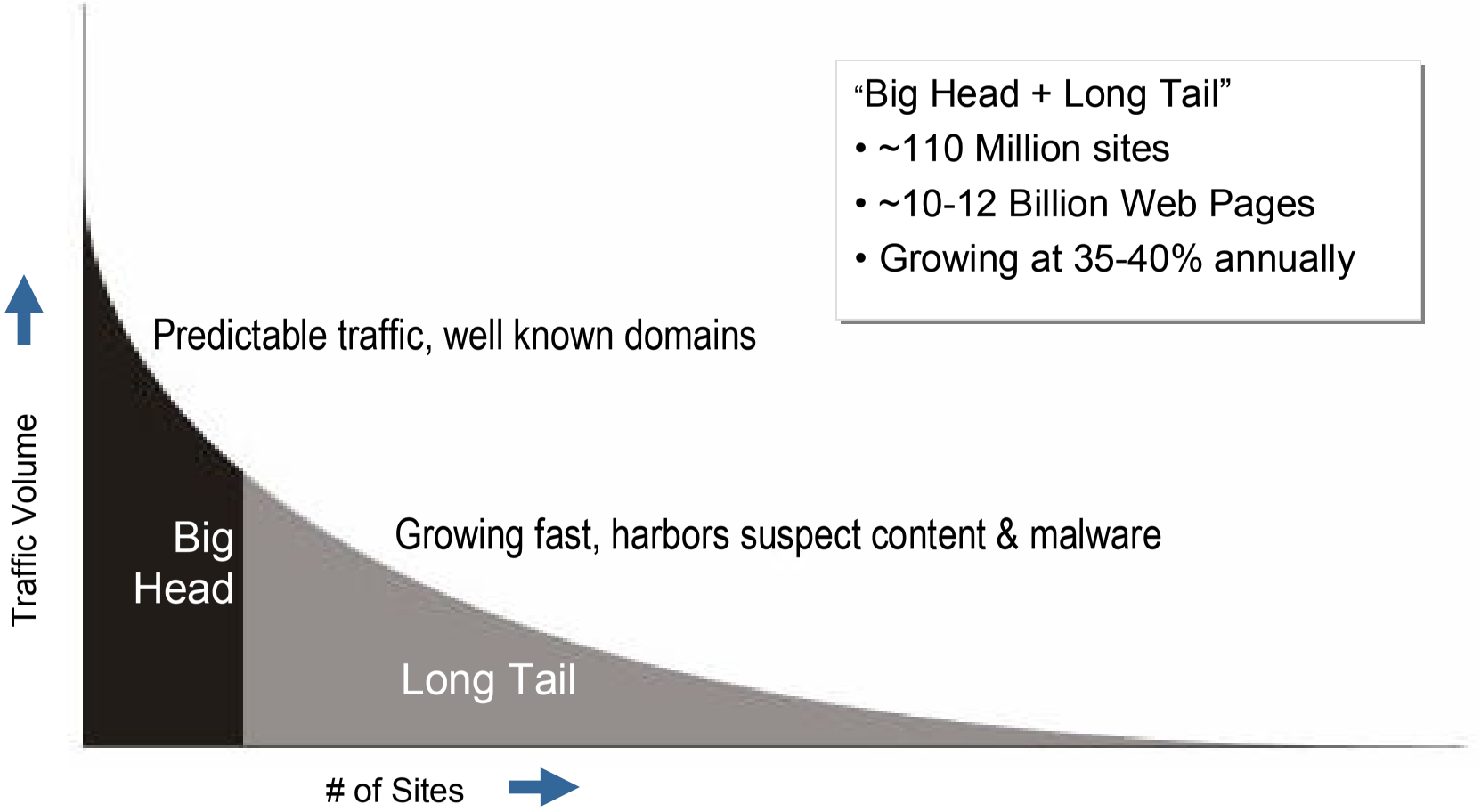
Web Traffic: Clear & Present Risks



- Over 75% of all Enterprises are infected with Spyware & Malware
- 35-40% of Web usage is non-business related (IDC Research)
- Malware threats & AUP violations result in compliance & legal exposure

Web Traffic

The Long Tail Gets Longer



IronPort S-Series

Addressing the Entire Spectrum of Web Traffic

IronPort Web Security Appliance

- Protects against known & unknown sites
- Best of breed signature scanning

Current Systems Not Designed for Today's Problems

- Low accuracy
- High latency / throughput
- Limited visibility to security threats

"Not the right tool for the job."

CISCO

IRONPORT

IronPort SenderBase Network

Largest Email & Web Traffic Monitoring Network

Largest: over 25% of traffic from 120,000+ sources

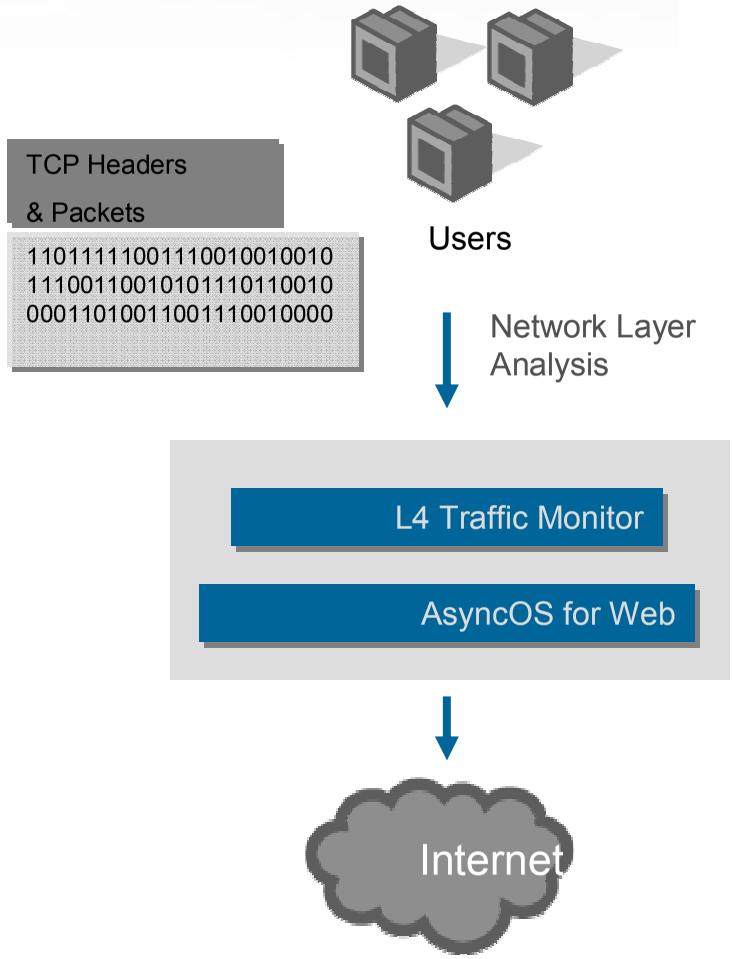
Broadest: 150 cross-protocol parameters

Best: Two year "head start" vs. alternative systems

Integrated L4 Traffic Monitor

Wire Speed Network Layer Scanning for Malware

- Scans all 65,535 ports at wire speed
- Detects rogue phone home activity
- Catches malware that attempts to bypass Port 80



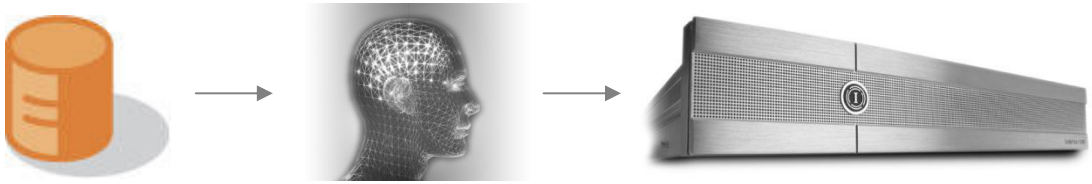
Web Reputation Filters

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 REALTIME



SenderBase Data

Data Analysis/ Security Modeling

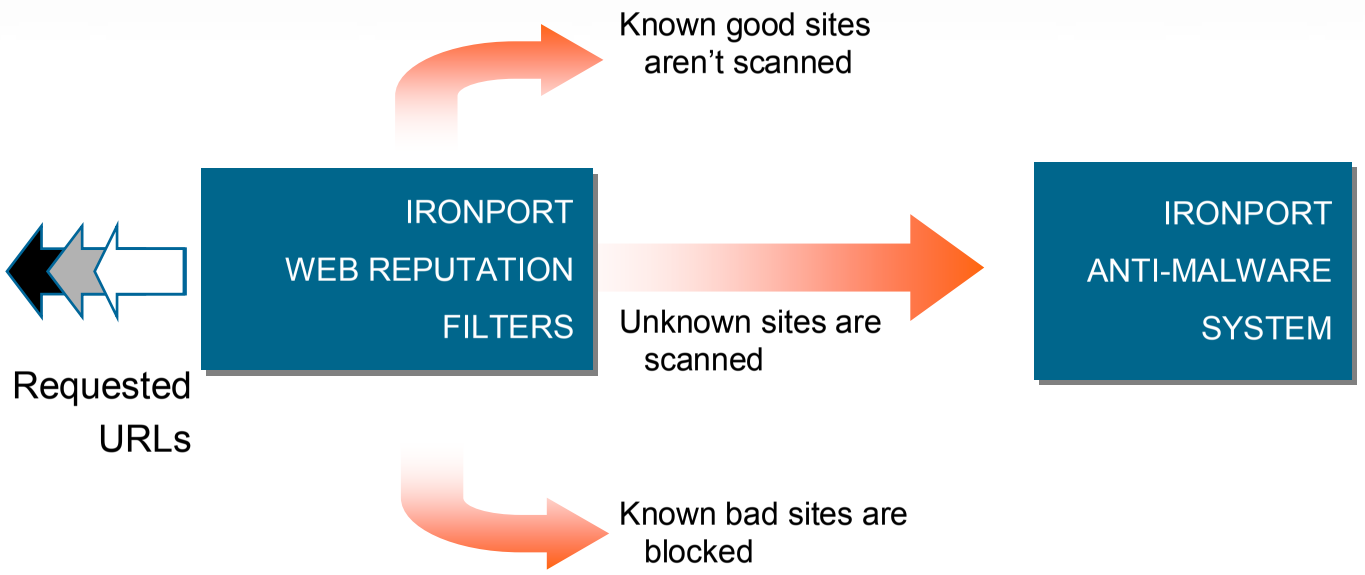
Web Reputation Scores (WBRS)

-10 to +10

CISCO

IRONPORT

Dynamic Application of Policies

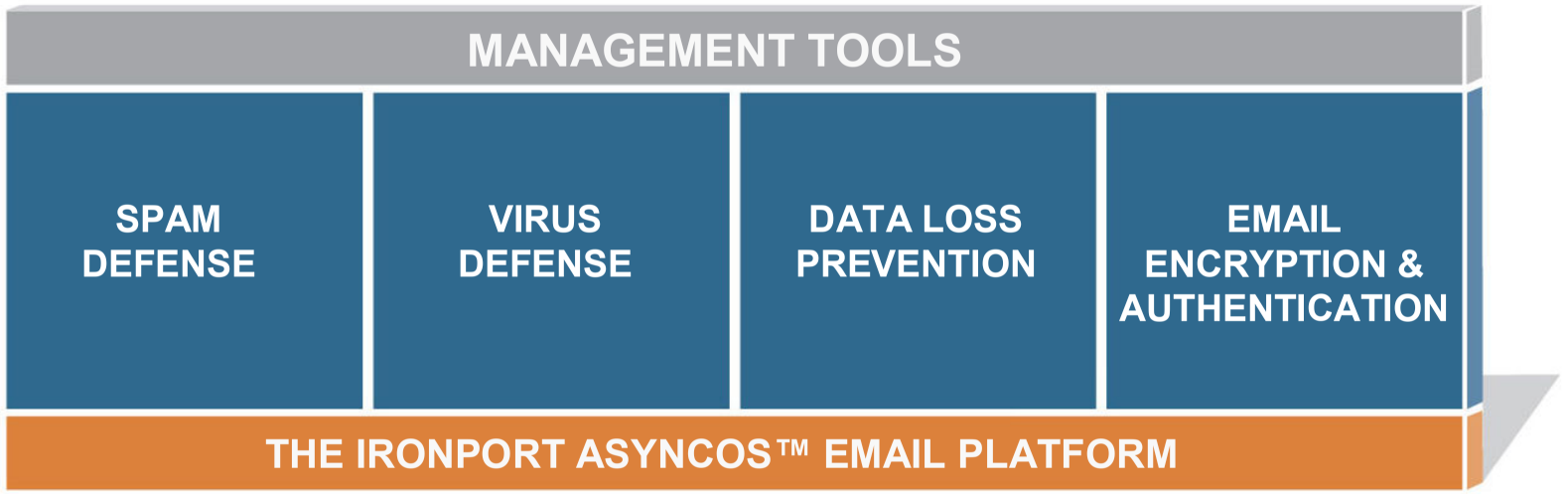


- **IronPort Web Reputation Filters** is a powerful *first* layer of defense
- **IronPort Anti-Malware System** provides a sophisticated *second* layer of defense

The Platform
IronPort AsyncOS

IronPort AsyncOS™

Unmatched Scalability and Security



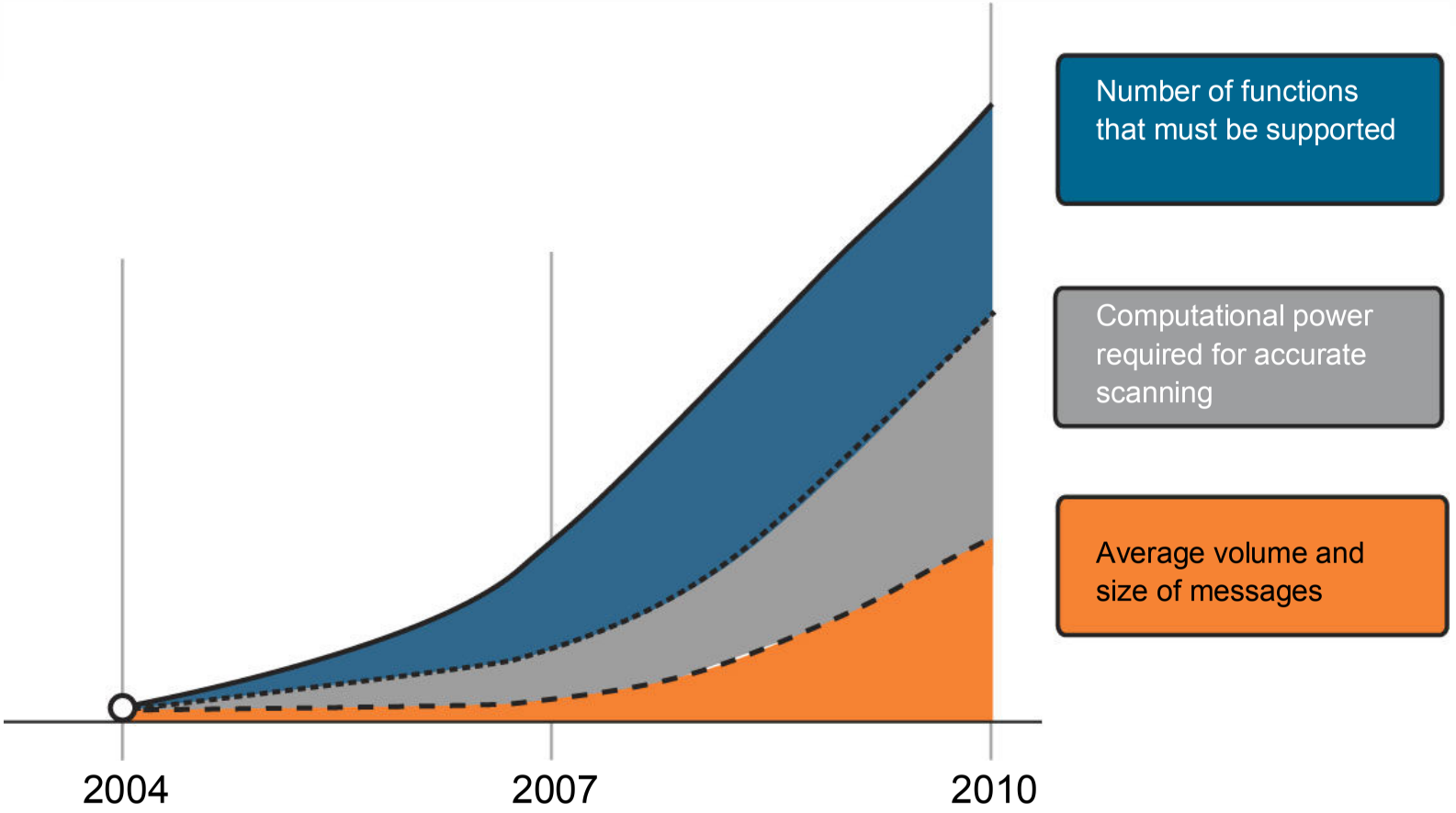
- **AsyncOS** scalable and secure OS optimized for messaging
- **Advanced Email Controls** protect reputation and downstream systems
- **Standards-based Integration** replaces legacy systems with ease

CISCO

IRONPORT

Scalable and Extensible Platform

Meeting Security Needs – Today and Tomorrow



IronPort AsyncOS

Revolutionary Email Delivery Platform

Traditional Email Gateways
And Other Appliances

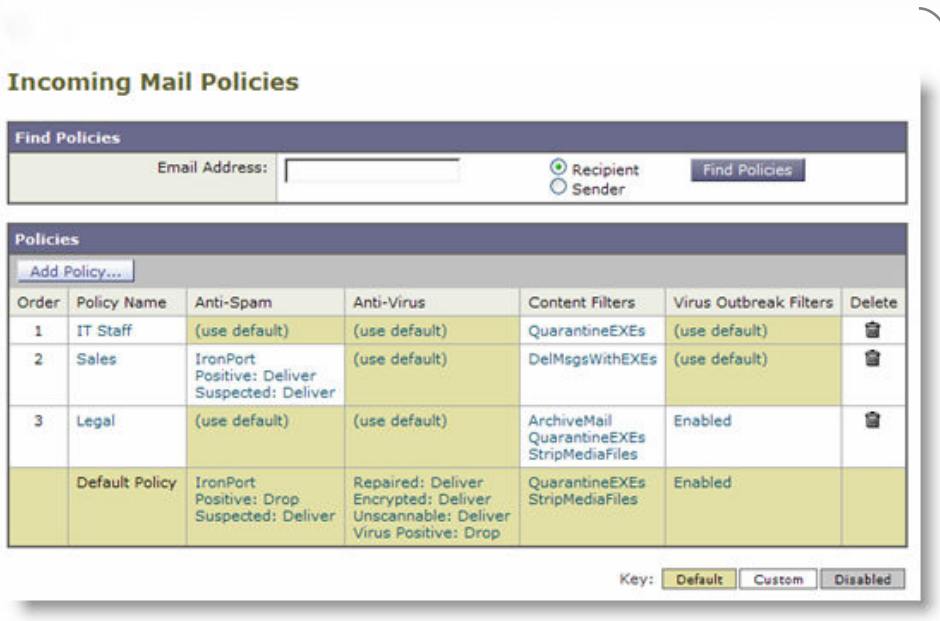
IronPort Email Security Appliances

200 Concurrent Connections	→	Low Performance/ Peak Delivery Issue	
Disk I/O Bottlenecks	→	Unable To Leverage Full Capability Components	
Single Queue for all destinations	→	Queue backup delays all email	

10.000 Concurrent Connections	→	High Performance/ Sure Delivery
CPU	→	Limited Solely By CPU Capacity
Per-Destination Queue	→	Fault-Tolerance and Custom Control

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

SALES

- Delete Executables

LEGAL

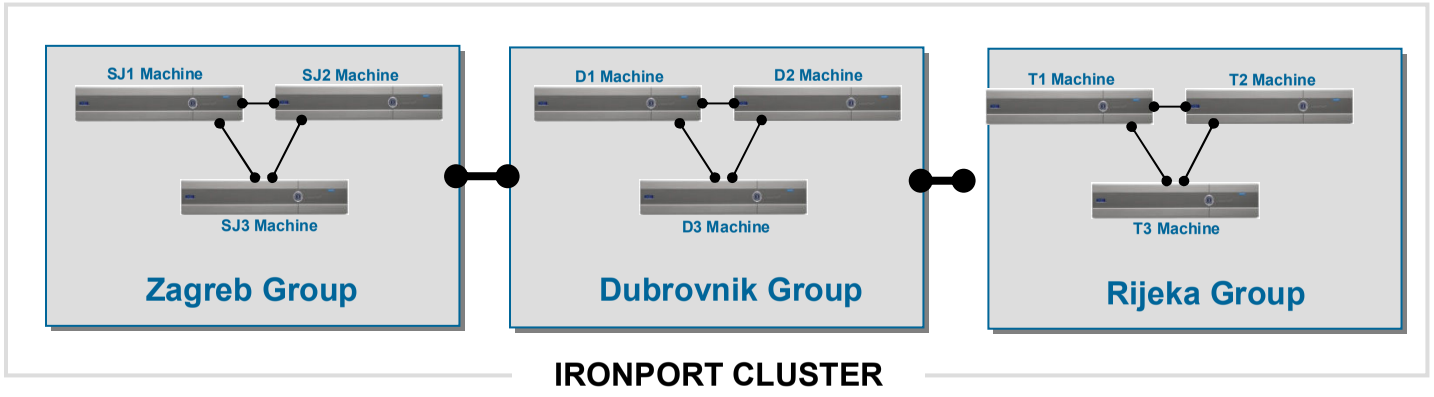
- Archive all mail
- Virus Outbreak Filters disabled for .doc files

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

IRONPORT®

IronPort Centralized Management

- Log in anywhere, control everywhere
- Interface assures configuration consistency
- Apply changes to a machine, group, or cluster
- Test on single system, “promote” to cluster



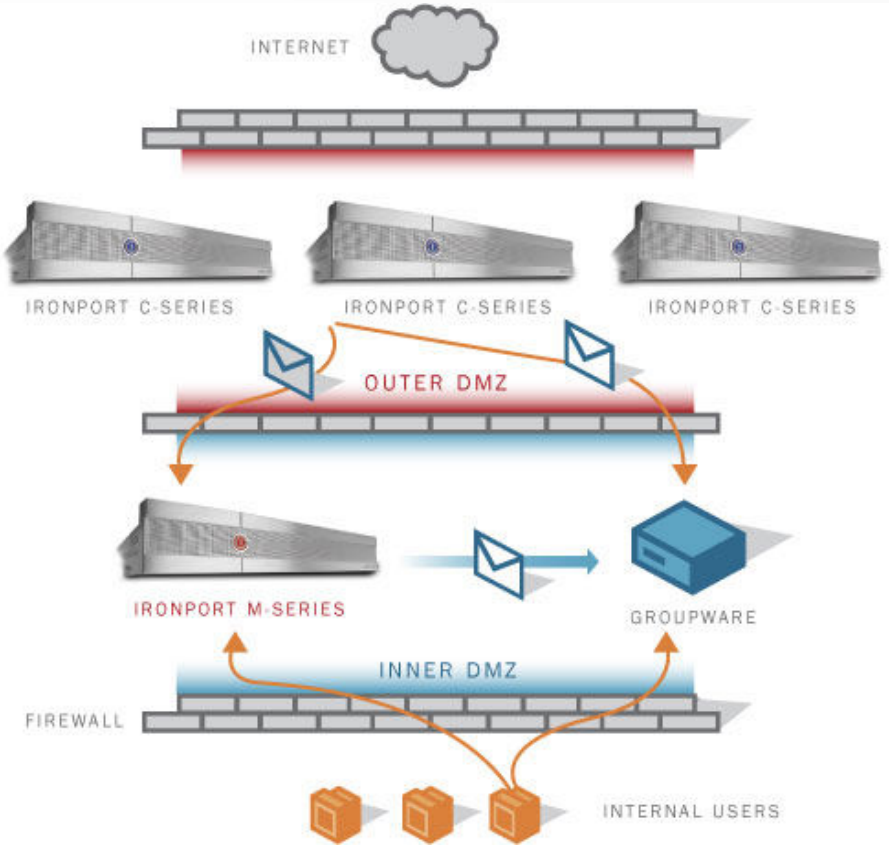
CISCO

IRONPORT

IronPort M-Series™

Security Management Appliances

- Centralized, self-managing quarantine appliance
- Provides complete end-user self-service, drives down administrator load
- Centralized Reporting and Message Tracking Console



cisco

IRONPORT

Sounds good? Test it!

- **Free evaluation for 30 days**
  - starts with activation of keys on unit
  - can be extended on request
- any size and any way
  - you get the right units for your needs
  - different ways of testing (life/ stealth, parallel, offline)
  - full support, full functionality
- About 85% of users who evaluate become happy customers!

cisco

IRONPORT

Get In Contact

IronPort, A Cisco Business Unit

Mirko Schneider
Territory Manager
Eastern Europe & Russia
Mobile: +49 172 83 96 04 7
mschneider@ironport.com

Hrvoje Dogan
Systems Engineer
Eastern Europe & Russia
Mobile: +385 917655625
hdogan@ironport.com

Distributor:
MACK IT
www.mack.hr
- partner contacts, evaluation equipment, technical specialists

CISCO

IRONPORT