



Cisco IronPort Perimeter Security Appliances



Tatjana Boskovic, Channel SE
tboskovi@cisco.com

Agenda

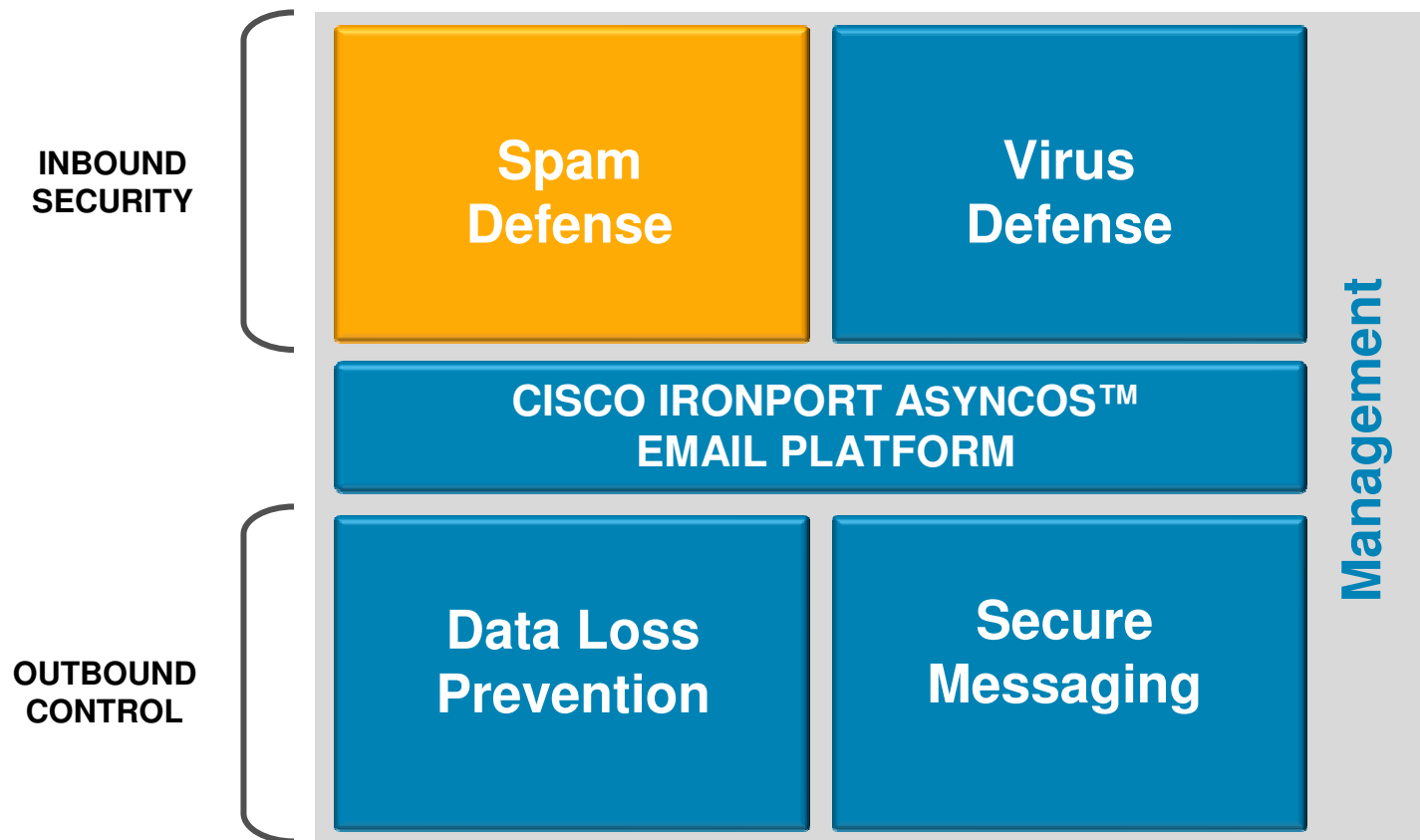
- Email security appliance
- Web security appliance
- Q&A

Email Security



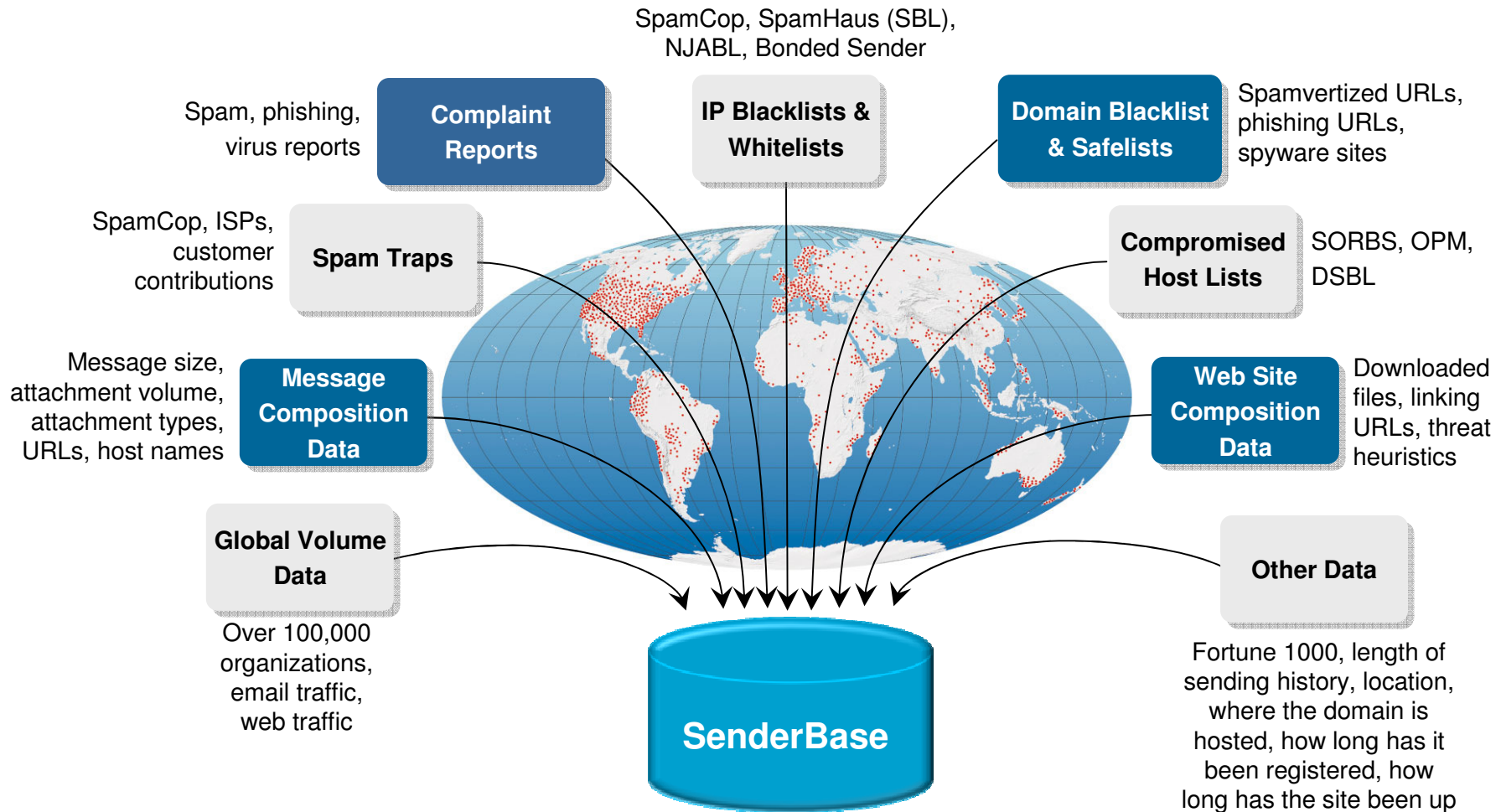
Email Security Architecture

Inbound Security, Outbound Control



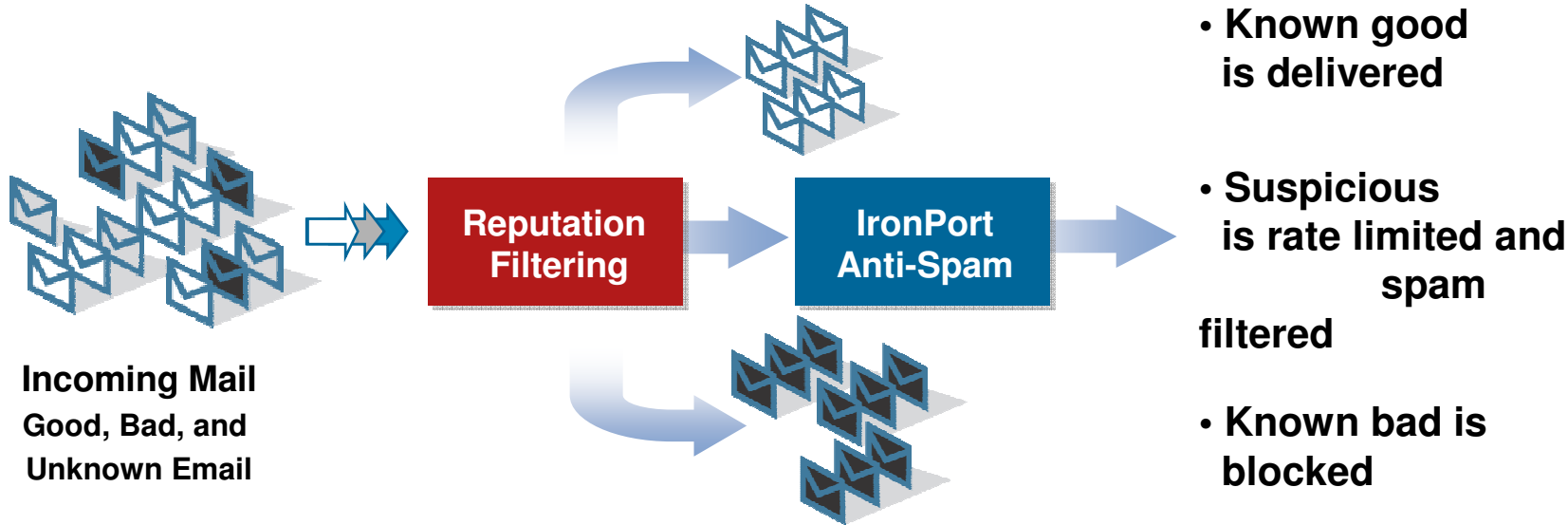
Cisco IronPort SenderBase

Breadth and Quality of Data Makes the Difference



SenderBase Reputation Filtering

Real Time Threat Prevention



Cisco on Cisco Our Corporate Email Experience

Message Category	%	Messages
Stopped by Reputation Filtering	93.1%	700,876,217
Stopped as Invalid recipients	0.3%	2,280,104
Spam Detected	2.5%	18,617,700
Virus Detected	0.3%	2,144,793
Stopped by Content Filter	0.6%	4,878,312
Total Threat Messages:	96.8%	728,797,126
Clean Messages	3.2%	24,102,874
Total Attempted Messages:		752,900,000

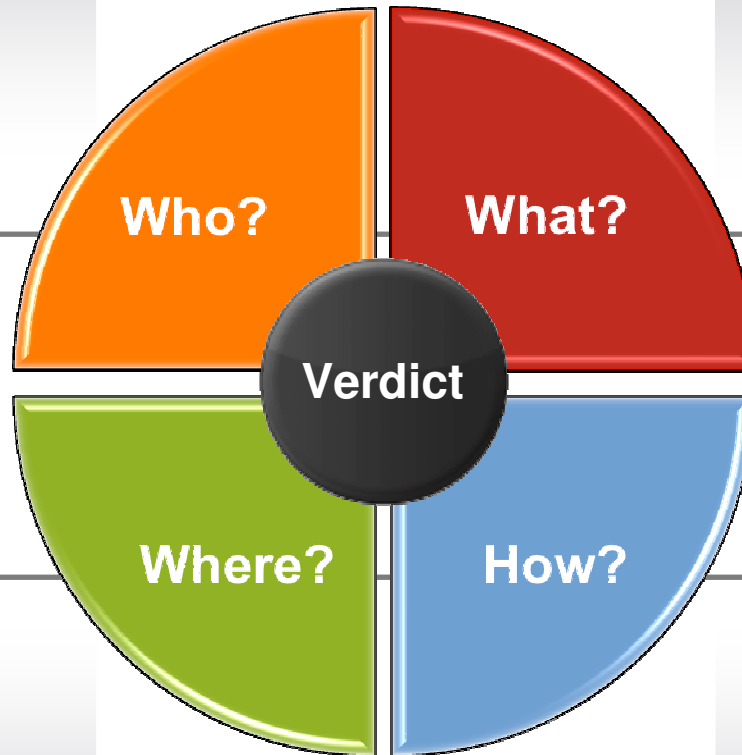
Cisco IronPort Anti-Spam

Defense in Depth Spam Protection



- ✓ Spam Botnets
- ✓ Spammer Networks

EMAIL REPUTATION



- ✓ SMS Spam
- ✓ Attachment-based Spam

MESSAGE CONTENT

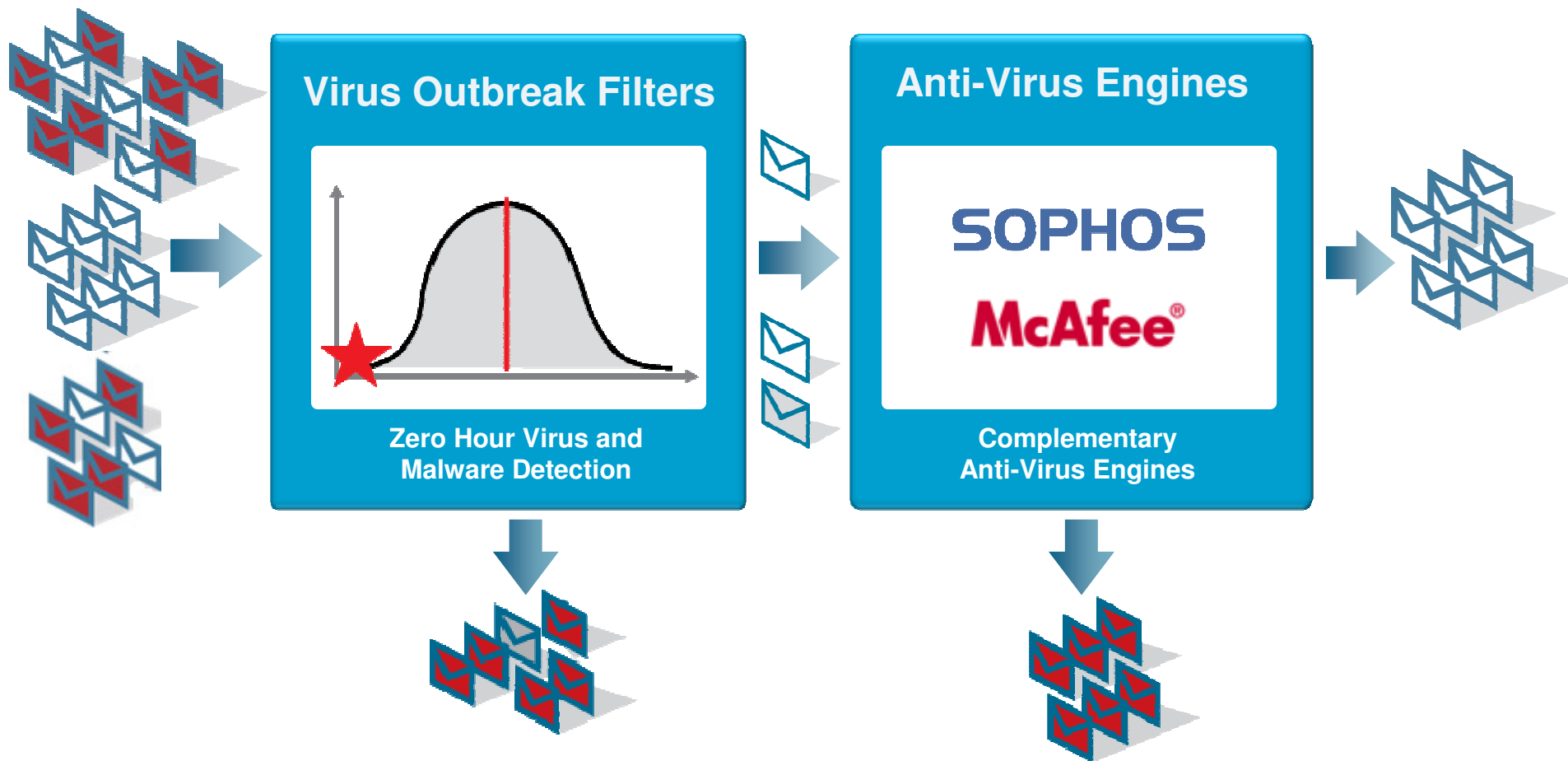
WEB REPUTATION

- ✓ Malware/Phishes
- ✓ Short-Texted Spam with URLs

MESSAGE CONSTRUCTION

- ✓ Image Spam
- ✓ Spam created using Automation Tools

Anti-Virus Defense in Depth



Data Loss Prevention

Simple Set Up

- Easy “3 click” set-up using content filters
- Use pre-defined content categories or create / customize your own
- Can be applied to specific users under specific conditions

Message Body or Attachment

Does the message body or attachment contain text that matches a specified pattern?

- Contains text:
 *
- Contains smart identifier:
ABA Routing Number
- Contains term in content dictionary:
HIPAA-Dictionary_txt

Number of matches required: (1-1000)

For content dictionaries, the number of matches is term weight.

Import from local computer:

Import from the *configuration* directory on your IronPort appliance

- GLBA-Dictionary.txt
- HIPAA-Dictionary.txt
- PCI-Dictionary.txt
- README
- SOX-Dictionary.txt
- config.dtd

Smart Identifiers: ?

Enable Smart Identifiers	Weight
<input checked="" type="checkbox"/> Credit Card Numbers	1
<input checked="" type="checkbox"/> Social Security Numbers	1
<input checked="" type="checkbox"/> ABA Routing Numbers	1
<input checked="" type="checkbox"/> CUSIPs	1

Data Loss Prevention

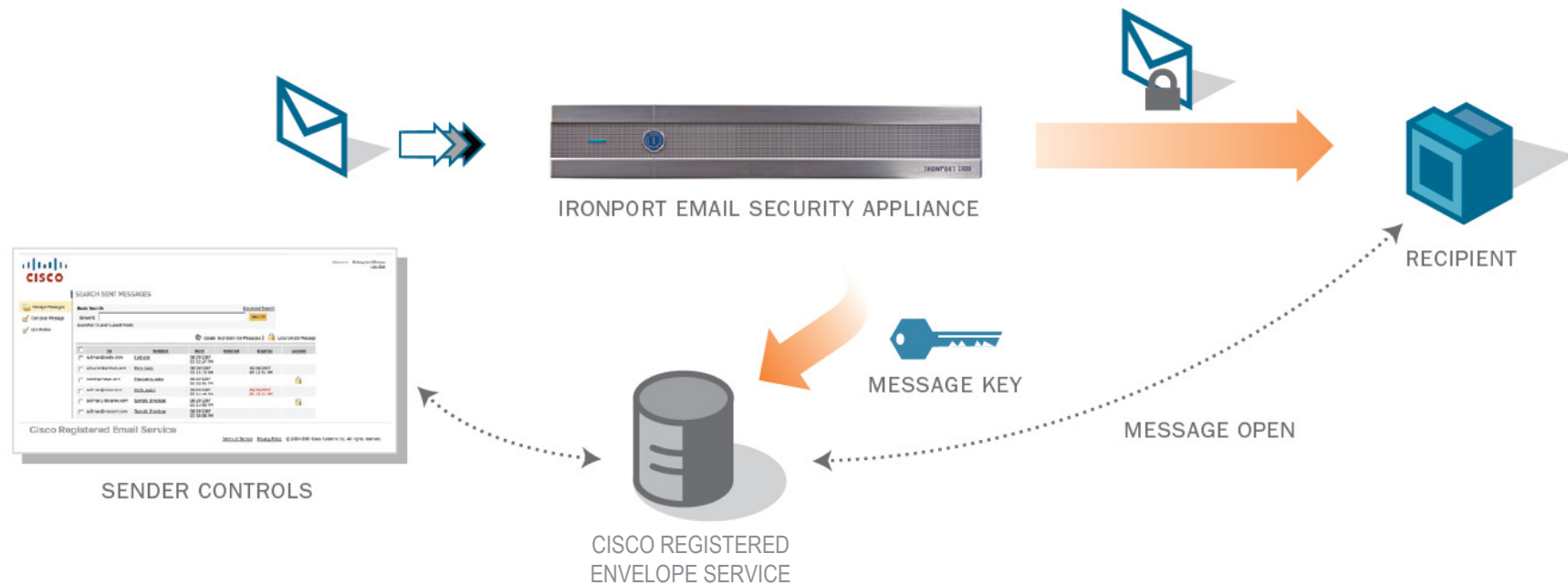
Comprehensive Remediation & Reporting

- Multiple remediation actions – encrypt, quarantine, drop, bounce, BCC, strip content
- Offending content highlighted in quarantine for easy analysis
- Reporting on a per policy and per user basis

The screenshot displays a remediation interface with two main panels. The left panel is a scrollable list of remediation actions, including 'Quarantine', 'Strip Attachment by Content', 'Strip Attachment by File Info', 'Add Disclaimer Text', 'Bypass Outbreak Filter Scanning', 'Send Copy (Bcc:)', 'Notify', 'Change Recipient to', 'Send to Alternate Destination Host', 'Deliver from IP Interface', 'Strip Header', 'Add Header', 'Encrypt and Deliver (Final Action)', 'Bounce (Final Action)', 'Deliver (Final Action)', and 'Drop (Final Action)'. The right panel provides a detailed view of the 'Quarantine' action, explaining that it flags the message to be held in one of the areas. It includes a dropdown menu for 'Send message to quarantine:' set to 'Policy', and a checkbox for 'Duplicate message' with a descriptive note: 'Send a copy of the message to the specified area. The original message will continue processing and the original message actions will apply to the original message.'

Cisco IronPort Email Encryption

Easy for the Sender. . .



- Automated key management
- No desktop software requirements
- Send to any email address seamlessly

Cisco IronPort Email Security Manager

Single view of policies for the entire organization

Incoming Mail Policies

Find Policies

Email Address: Recipient Sender

Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	IT Staff	(use default)	(use default)	QuarantineEXEs	(use default)	
2	Sales	IronPort Positive: Deliver Suspected: Deliver	(use default)	DelMsgsWithEXEs	(use default)	
3	Legal	(use default)	(use default)	ArchiveMail QuarantineEXEs StripMediaFiles	Enabled	
	Default Policy	IronPort Positive: Drop Suspected: Deliver	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	QuarantineEXEs StripMediaFiles	Enabled	

Key:

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

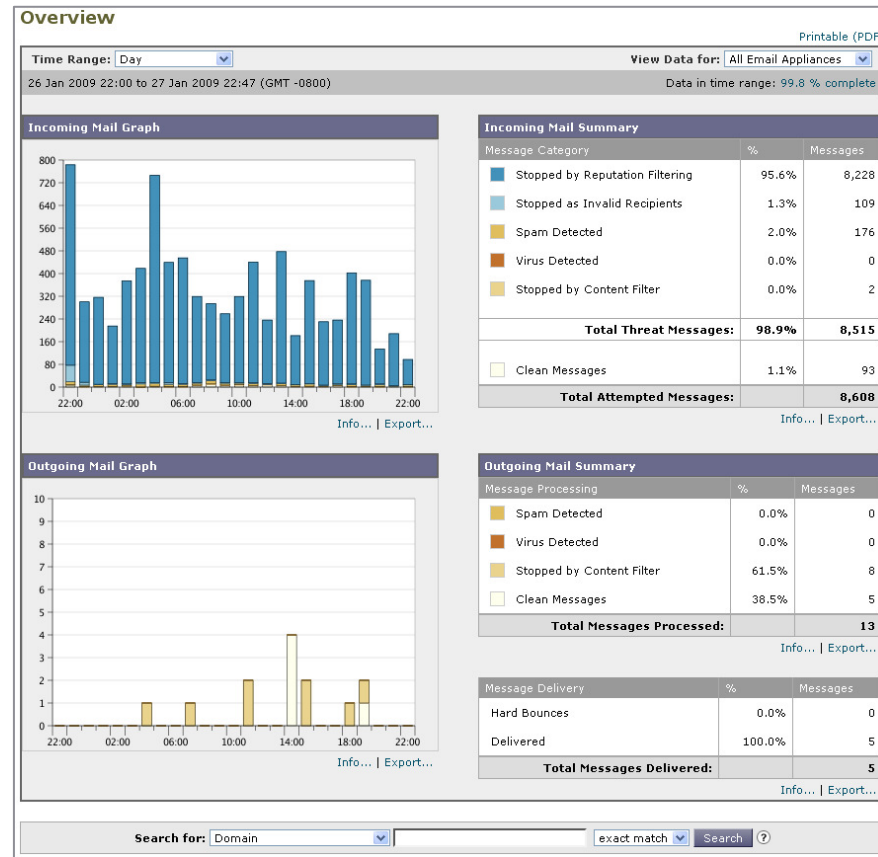
“IronPort Email Security Manager serves as a single, versatile dashboard to manage all the services on the appliance.” – PC Magazine

Comprehensive Insight

Unified Business Reporting

Consolidated Reports

- Single view across the organization
- Real Time insight into email traffic and security threats
- Actionable drill down reports



Multiple data points

Virus Outbreaks smtp.spartanmail.net

26 Jan 2009 22:00 to 27 Jan 2009 22:47 (GMT -0800) Data in time range: 99.8 % complete

Outbreak Source	Outbreak Message	Outbreak Type	Outbreak Count
Outbreak Source	Outbreak Message	Outbreak Type	Outbreak Count
Outbreak Source	Outbreak Message	Outbreak Type	Outbreak Count

Outbreak Details

Outbreak Name	Origin	First Seen	Message Type	Outbreak Count
Outbreak Name	Origin	First Seen	Message Type	Outbreak Count
Outbreak Name	Origin	First Seen	Message Type	Outbreak Count

- Email Volumes
- Spam Counters
- Policy Violations
- Virus Reports
- Outgoing Email Data
- Reputation Service
- System Health View

Internal Users smtp.spartanmail.net

26 Jan 2009 22:00 to 27 Jan 2009 22:47 (GMT -0800) Data in time range: 99.8 % complete

Internal User	Internal User	Internal User	Internal User	Internal User	Internal User
Internal User	Internal User	Internal User	Internal User	Internal User	Internal User
Internal User	Internal User	Internal User	Internal User	Internal User	Internal User

Visibility Into Email Messages

Message Tracking

What happened to the email I sent 2 hours ago?

- ✓ Track Individual Email Messages

Who else received similar emails?

- ✓ Forensics to Ensure Compliance

The screenshot shows the 'Message Tracking' search interface. At the top, it displays the 'Available Time Range' from 08 Oct 2007 09:10 to 27 Jan 2009 22:51 (GMT -0800) and indicates that 'Data in time range: 91.25% complete'. The search criteria are organized into several sections: 'Envelope Sender', 'Envelope Recipient', and 'Subject', each with a 'Begins With' dropdown menu. The 'Message Received' section includes radio buttons for 'Last Day', 'Last Week', and 'Custom Range'. The 'Custom Range' is set for 'Start Date: 01/26/2009 22:00' and 'End Date: 01/27/2009 22:52 (GMT -0800)'. Below this is an 'Advanced' section with a 'Sender IP Address' field and radio buttons for 'Search rejected connections only' and 'Search messages'. The 'Message Event' section includes a note about selecting multiple events and a list of checkboxes for 'Virus Positive', 'Spam Positive', 'Suspect Spam', 'Delivered', 'Hard bounced', 'Soft bounced', 'Currently in Outbreak Quarantine', and 'Quarantined as Spam'. Other fields include 'Message ID Header', 'IronPort MID', and 'IronPort Host' (set to 'All Hosts'). At the bottom, there are 'Query Settings' for 'Query timeout: 1 minute' and 'Max. results returned: 250'. 'Clear' and 'Search' buttons are located at the bottom left and right respectively.

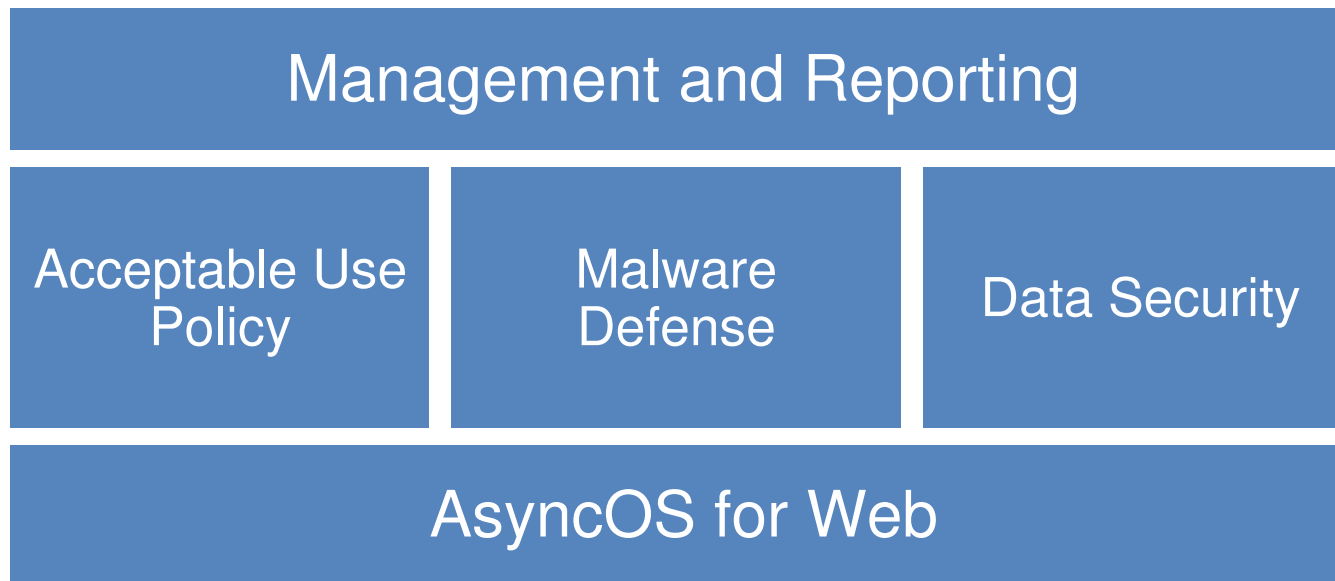
Web Security



Cisco IronPort S-Series

A Powerful, Secure Web Gateway Solution

- Most effective defense against web-based malware
- Visibility and control for acceptable use and data loss
- High performance to ensure best end-user experience
- Integrated solution offering optimum TCO



Customer Problem

**The
Categorized
Web**

20% covered by URL lists

The Dark Web

*80% of the web is
uncategorized, highly
dynamic or unreachable*

- Dynamic content*
- Password protected sites*
- User generated content*
- Short life sites*

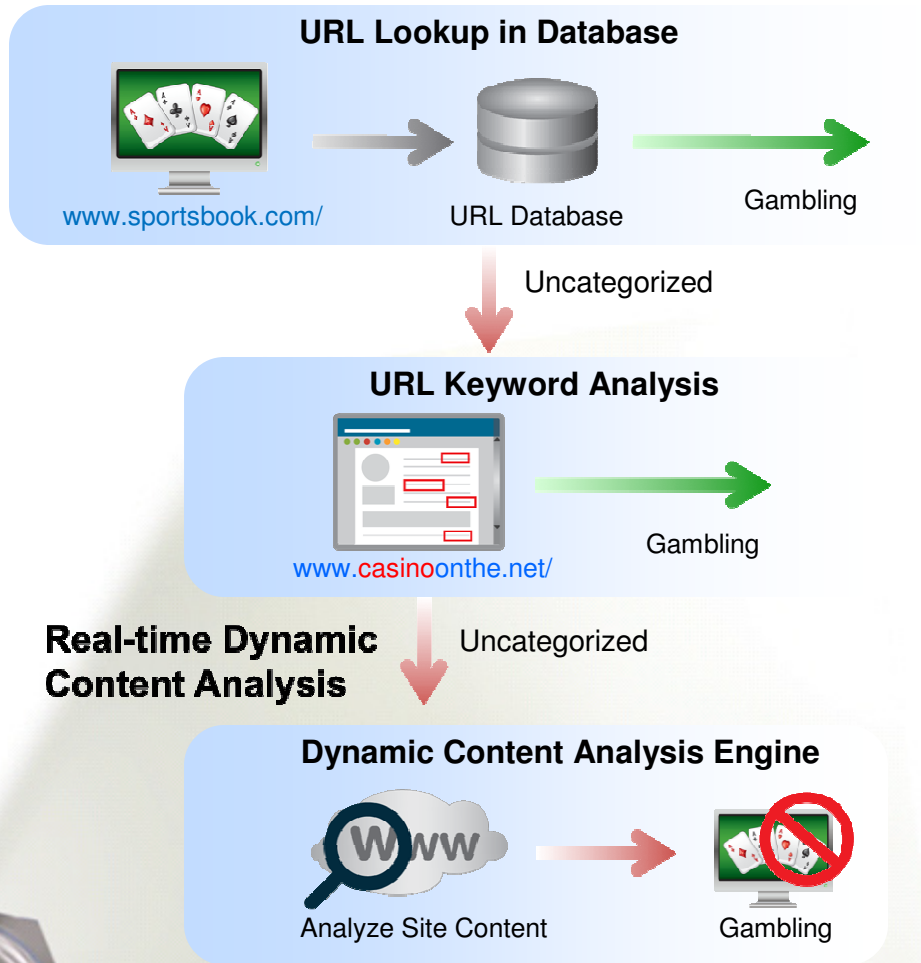


The Categorized Web

20% covered by URL lists

Introducing Cisco IronPort Web Usage Controls

A Spotlight for the Dark Web



- Industry-leading URL database efficacy
 - 65 categories
 - Updated every 5 minutes
 - Powered by Cisco SIO
- Real-time Dynamic Content Analysis Engine accurately identifies over 90% of Dark Web content in commonly blocked categories



How Does the DCA Engine Work?

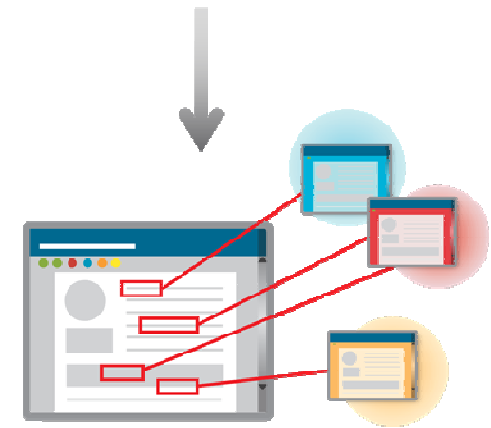
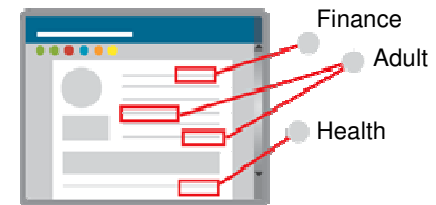
1. User requests unknown webpage.



2. HTTP response received. Scan response to **identify relevant text**.

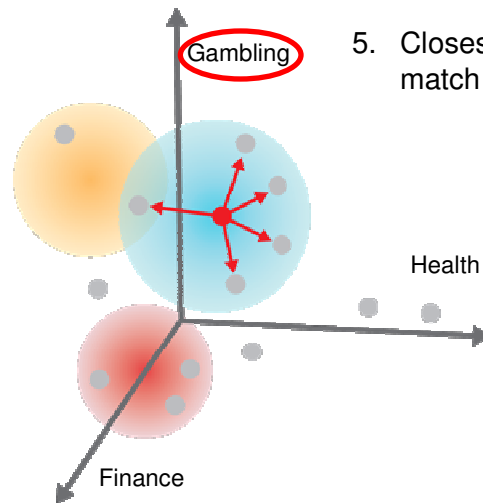


3. Calculate **content vector**. Each dimension is a score of the document's relevance to a particular category.



4. Calculate proximity of document's vector to the vectors of **model documents**.

5. Closest category match is returned.

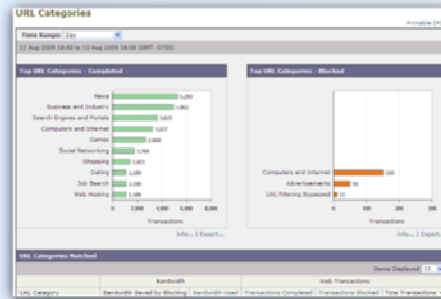
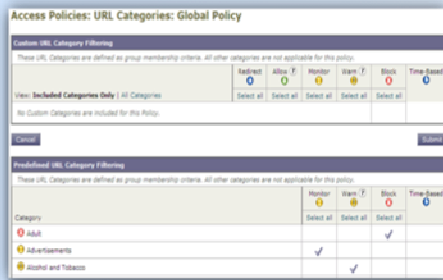


6. Policy for category match is enforced: Block / Allow / Warn.



Cisco IronPort Web Usage Controls

Leading Efficacy, Rich Controls, Comprehensive Visibility



Control

- Per user, per group policies
- Multiple actions: block, warn, monitor
- Time-based policies
- Unlimited custom categories
- Custom end-user notifications

Visibility

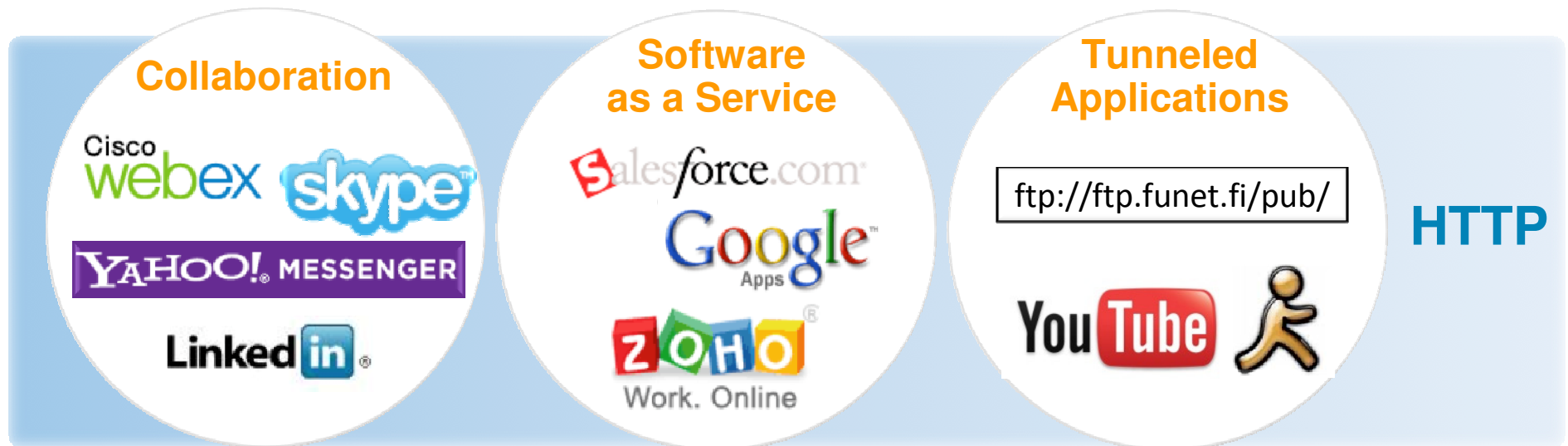
- Easy to understand reports
- Extensive logging
- Comprehensive alerting

Efficacy

- 200+ countries
- 50+ languages
- 65 categories
- Less than 1 in 1 million false positives

Web Application Control

- Native control for HTTP, HTTP(s), FTP applications
- Selective decryption of SSL traffic for security and policy
- Policy enforcement for applications tunneled over HTTP—FTP, IM, video
- Application traversal using policy-based HTTP CONNECT



Integrated Identity and Authentication

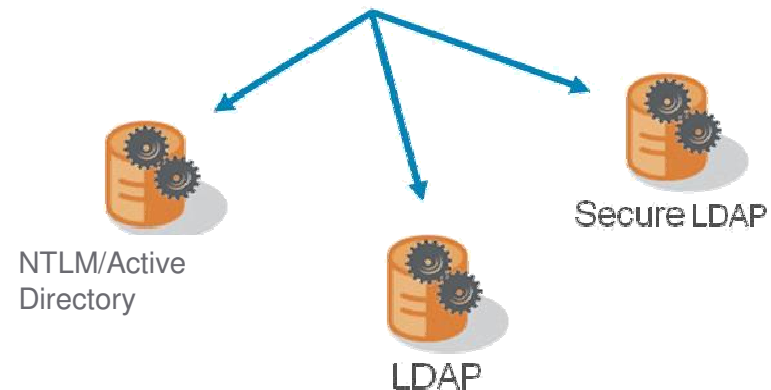
User-Specific Acceptable Use and Data Security Policies

- Authentication against LDAP servers
- Transparent, single sign-on (SSO) authentication against Active Directory
- Multi-realm sequencing
- Multi-domain authentication
- Guest policies
- Re-Auth and Failed Auth policies

Access Policies

Policies						
Order	Group	Applications	URL Categories	Objects	Web Reputation and Anti-Malware Filtering	Delete
1	Sales Policy Identity: Sales	Block: FTP over HTTP Allow: HTTP, HTTPS, Native FTP Allow: Ports 20, 21,....	Redirect: 0 Allow: 0 Monitor: 36 Warn: 0 Block: 14 Need: 3	Block: Object Types HTTP/HTTPS Object Max Size: None FTP Object Max Size: None	(global policy)	
2	Technical Groups Policy Identity: Engineering	(global policy)	0	(global policy)	(global policy)	
	Global Policy Identity: All	Allow: FTP over HTTP, HTTP, ... Allow: Ports 8080, 21,....	Allow: U Monitor: 37	HTTP/HTTPS Object Max Size: None FTP Object Max Size: None	(enabled)	

Integrated Authentication



Define Acceptable Use and Data Security Policies using Rich Identity Constructs

Multi-Layered Malware Defense

Protection Against Today's Threats



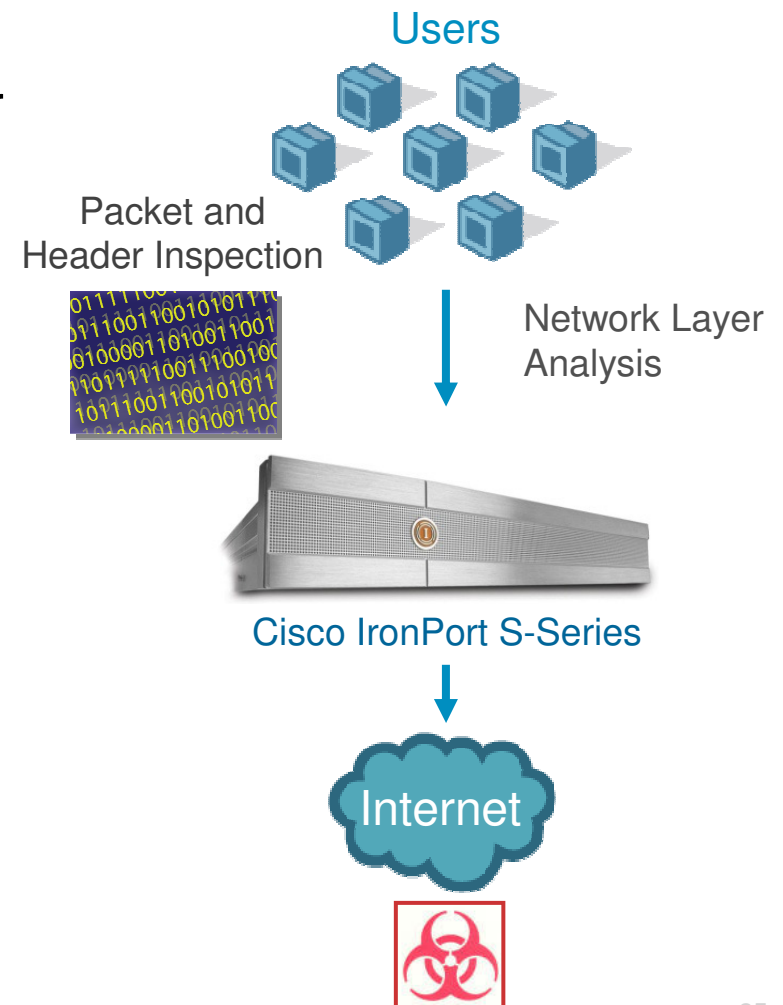
- Detects malicious botnet traffic across all ports
- Blocks 70 percent of known and unknown malware traffic at connection time
- Blocks malware based on deep content analysis



Detecting Existing Client Infections

Preventing “Phone-Home” Traffic

- Cisco IronPort Layer 4 Traffic Monitor
 - Scans all traffic, all ports, all protocols
 - Detects malware bypassing Port 80
 - Prevents botnet traffic
- Powerful anti-malware data
 - Automatically updated rules
 - Real-time rule generation using “Dynamic Discovery”



Web Reputation Filters

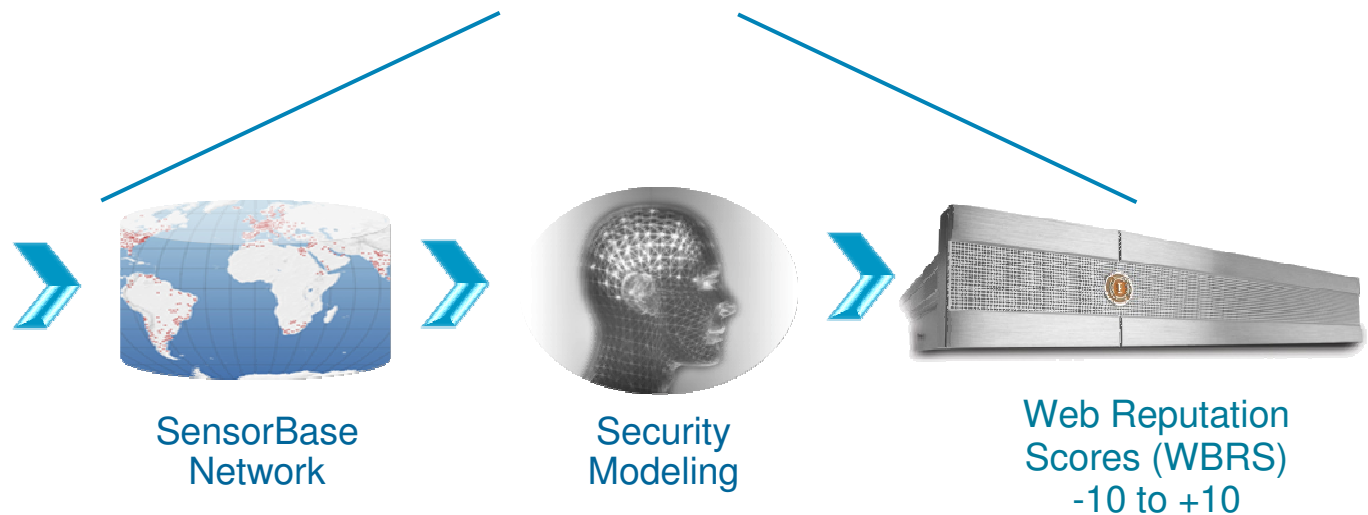
Predictive, Real-Time Threat Prevention



200+ Parameters

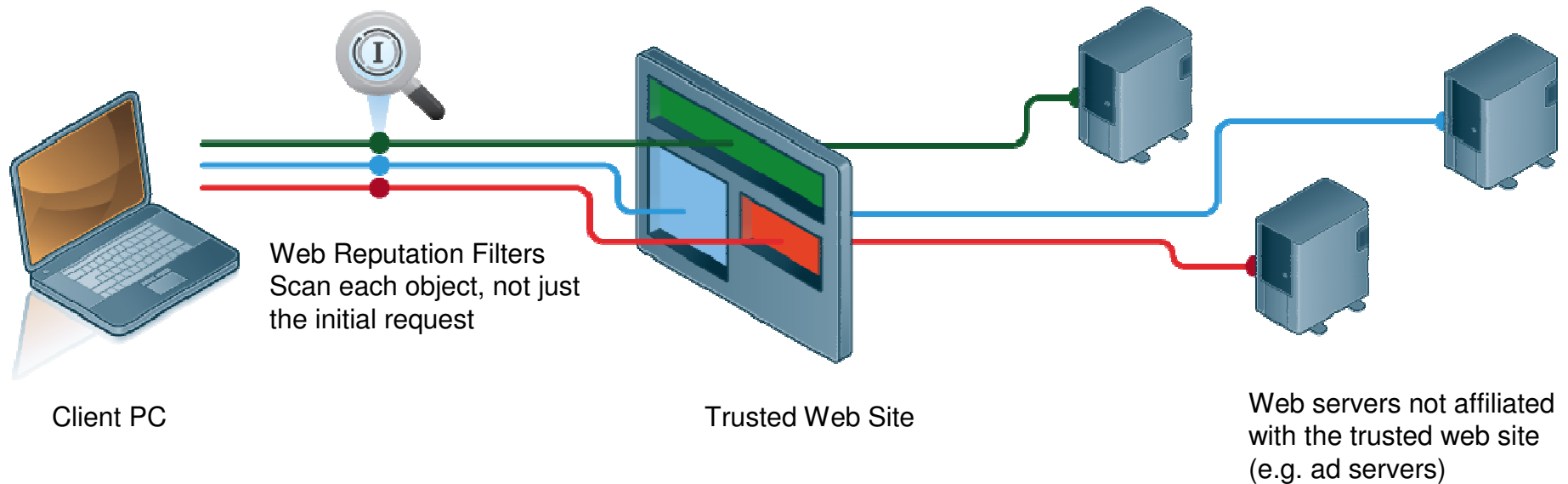
- URL Blacklists
- URL Whitelists
- Dynamic IP Addresses
- Bot Networks
- URL Behavior
- Global Volume Data
- Domain Registrar Information
- Compromised Host List
- Real-Time Cloud Analysis
- Network Owners
- Known Threat URLs

Cisco Security Intelligence Operations



Protection For a Dynamic Web 2.0 World

Visibility Beyond the Initial Threat



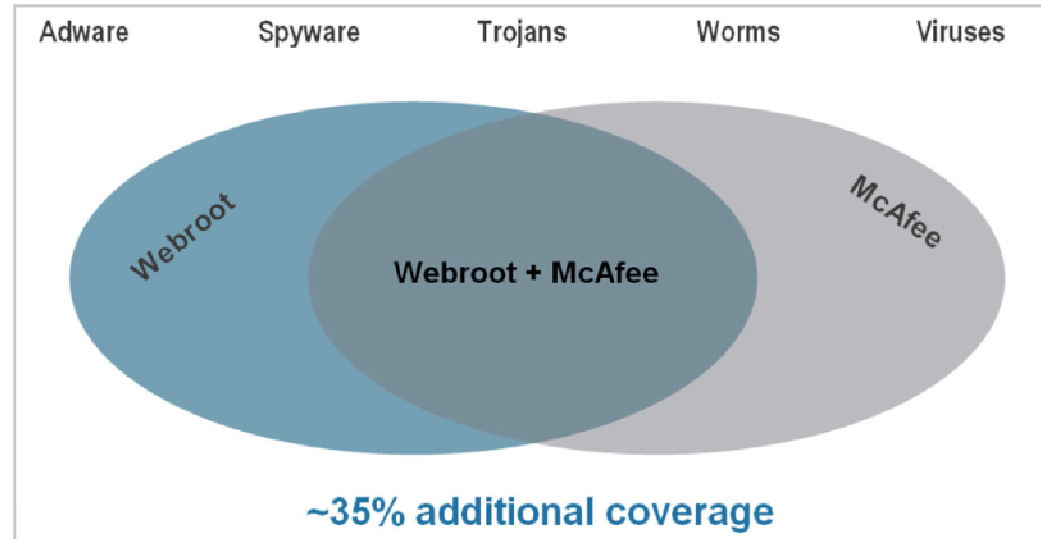
- Web pages are made up of objects coming from different sources
- Objects can be images, executables, JavaScript...
- Compromised websites often grab malicious objects from external sources
- Security means looking at each object individually, not just the initial request

Cisco IronPort DVS Engine

Dynamic Vectoring and Streaming



- Accelerated signature scanning
 - Parallel scans
 - Stream scanning
- Multiple integrated verdict engines
 - McAfee and Webroot
- Automated updates
- Decrypt and scan SSL traffic
 - Selectively, based on category and reputation



Data Security




On-box Common Sense Security

- Content metadata inspection, along with visibility and forensics
- Allow, block, log
 - Based on file metadata, URL category, user and web reputation
- Multi-protocol
 - HTTP(s), FTP, HTTP tunneled



Common Sense Policies

Simple Approach for Avoiding Web Data Breaches

Who?	John Smith, Finance	John Smith, Finance	Jane Doe, Sales
What?	FiscalPlan.xls	FiscalPlan.xls	CustomerList.doc
Where?	Webmail.com	Taxfirm.com	Personal-site.com, -9 Reputation score
How?	HTTPS (Encrypted)	HTTPS (Encrypted)	FTP
Verdict			

Cisco IronPort Web Security Manager

Single View of Policies for the Entire Organization

Web Filtering Policies

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



Marketing

- Block FTP uploads
- Allow media files
- Route requests to partner site



Sales

- Block executables
- Block sports sites 9am-5pm M-F
- Decrypt HTTPS connections

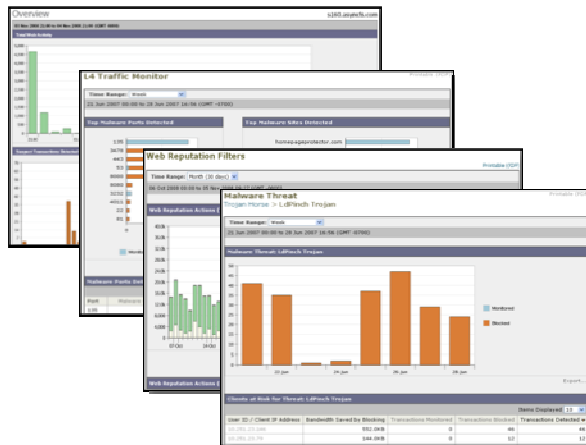


IT

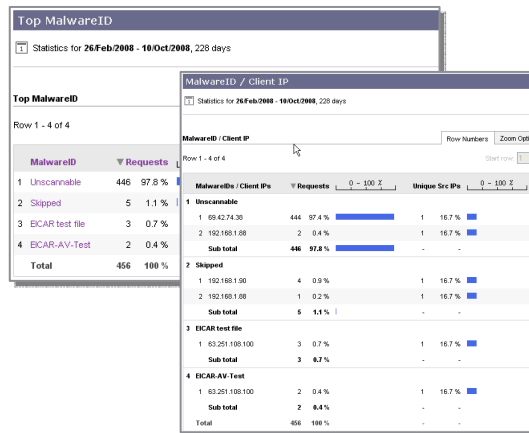
- Allow all URL categories
- Exempt Adobe updates from authentication
- Block all malware

Configure granular policies based on a variety of parameters

Comprehensive Security Reporting



- In-depth threat visibility
 - Web Traffic Overview
 - Layer 4 Traffic Monitor
 - Anti-Malware Category and Threat Details
 - Client Malware Risk
 - Client Activity Detail
 - Web Reputation Filters
 - Website Activity and Detail



- Detailed off-box analysis
 - Offload extensive data crunching
 - Top N and trend reporting for malware
 - Client, Source, Malware Name and Category



System Monitoring

Easy Integration with Existing Processes



Alert Center

Alert Recipients							
Add Recipient...							
Recipient Address	System	Hardware	Updater	Web Proxy	DVS and Anti-Malware	L4 Traffic Monitor	Delete
sng@ironport.com	All	All	All	All	All	All	

Alert Settings	
From Address to Use When Sending Alerts:	Automatically Generated
Initial Number of Seconds to Wait Before Sending a Duplicate Alert:	300
Maximum Number of Seconds to Wait Before Sending a Duplicate Alert:	3600
IronPort AutoSupport:	Enabled
Send copy of weekly AutoSupport reports to System Information Alert recipients.	
Edit Settings...	

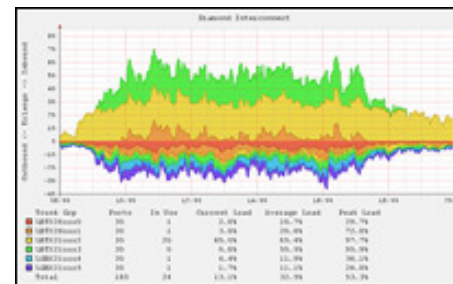
- Alert subscriptions per administrator
- Distinct areas of management

Log Subscriptions

Configured Log Subscriptions				
Add Log Subscription...				
Log Name	Type	Log Files	Rollover	Delete
accesslogs	Access Logs	ftp://wsa07.wga/accesslogs	<input type="checkbox"/>	
cli_logs	CLI Audit Logs	ftp://wsa07.wga/cli_logs	<input type="checkbox"/>	
gui_logs	GUI Logs	ftp://wsa07.wga/gui_logs	<input type="checkbox"/>	
logderrorlogs	Logging Logs	ftp://wsa07.wga/logderrorlogs	<input type="checkbox"/>	
proxylogs	Proxy Logs	ftp://wsa07.wga/proxylogs	<input type="checkbox"/>	
reportlogs	Reporting Logs	ftp://wsa07.wga/reportlogs	<input type="checkbox"/>	
reportquery_logs	Reporting Query Logs	ftp://wsa07.wga/reportquery_logs	<input type="checkbox"/>	
shd_logs	SHD Logs	ftp://wsa07.wga/shd_logs	<input type="checkbox"/>	
system_logs	System Logs	ftp://wsa07.wga/system_logs	<input type="checkbox"/>	
trafmon_errlogs	Traffic Monitor Error Logs	ftp://wsa07.wga/trafmon_errlogs	<input type="checkbox"/>	
trafmonlogs	Traffic Monitor Logs	ftp://wsa07.wga/trafmonlogs	<input type="checkbox"/>	
updater_logs	Updater Logs	ftp://wsa07.wga/updater_logs	<input type="checkbox"/>	
wbnp_logs	WBNP Logs	ftp://wsa07.wga/wbnp_logs	<input type="checkbox"/>	
wbrs_logs	WBRs Logs	ftp://wsa07.wga/wbrs_logs	<input type="checkbox"/>	
webrootlogs	Webroot Logs	ftp://wsa07.wga/webrootlogs	<input type="checkbox"/>	

- Squid, Apache, W3C, custom log formats
- Delivery via SCP, syslog, FTP

SNMP



- Exclusive IronPort MIB
- Integrates with any SNMP-compatible tools
- SNMP v1, v2, v3

Right-Sized Hardware Platforms

Remote Office and Back Office (ROBO) to Enterprise

Capacity and Throughput

- Multiple network integration options (transparent L4 re-direction options, PAC file, WPAD, WCCP)
- Built-in system redundancy – RAID 10, dual power supplies
- High availability – WCCP, DNS, L4
- Flexible network routing

Cisco IronPort S160

1-1,000 users



Cisco IronPort S360

1,000-10,000 users



Cisco IronPort S660

10,000-30,000 users



ROBO

Regional HQ / Mid-Market

Corporate HQ

Market Segment

Cisco Secure Web Gateway

Industry's Highest-Performance Integrated Solution

Secure

Multi-layered malware defense

Web reputation filters

Accelerated signature scanning (DVS engine)

Prevent botnets and malware bypassing Port 80 (L4TM)

Control

Integrated authentication and SSO

Enterprise-class URL filtering

Applications and object filtering

Web usage visibility and tracking

Prevent

On-box simple data security

Off-box interoperability with third-party DLP

Prevent malware-initiated data breaches (L4TM)



95% of companies who try Cisco IronPort become customers.

Contact us!

