



# Latest Internet threats & reputation-based security solutions



**Sébastien Commérot**  
**Manager, IronPort Marketing**

Cisco IronPort  
Central & Eastern Europe, Latin America, Middle-East & Africa

# Cisco IronPort

## Unparalleled Market Leadership

### Gartner

*IronPort Positioned in the “Leaders”  
Quadrant in Magic Quadrant Report*



*IronPort is positioned as a leading  
player in the messaging security  
appliance market*

**THE RADICATI GROUP, INC.**  
A TECHNOLOGY MARKET RESEARCH FIRM

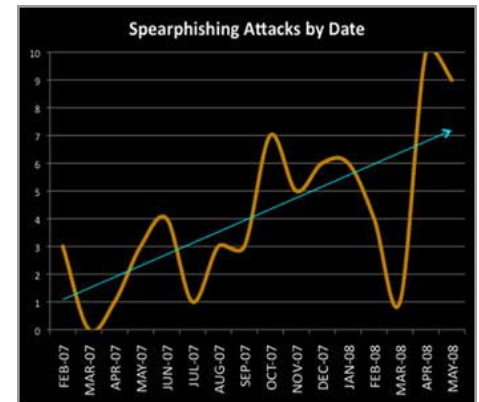
*Named IronPort the market share  
leader in the email security appliance  
market*

- IronPort funded in 2000, acquired by Cisco in 2007
- 20,000+ customers globally
- 400 million users protected
- 40% of Fortune 100 companies
- 8 of the 10 largest service providers
- 99%+ customer renewal rates

# Phishing is changing



- 1/3 of phishing sites host malware
- Average on-line time for a phishing site: 3 days



Source : Anti-Phishing Working Group

# What about TypoSquatting?

- Focus on heavy traffic sites
- Hackers register names close to famous brands or sites
  - Inve~~s~~rion of 1 letter
  - Name variant  
(micr~~p~~soft)
  - Orthogra~~f~~ic Mistake
- Creation of a similar site, downloading malware on computers

[www.google.com](http://www.google.com)

[www.mcrosoft.com](http://www.mcrosoft.com)

[www.hotmial.com](http://www.hotmial.com)

[www.wikipedia.org](http://www.wikipedia.org)

# Zombies are changing

## The Storm network

- **The world's most important botnet**

1000 contaminated PCs rented \$220 in Germany

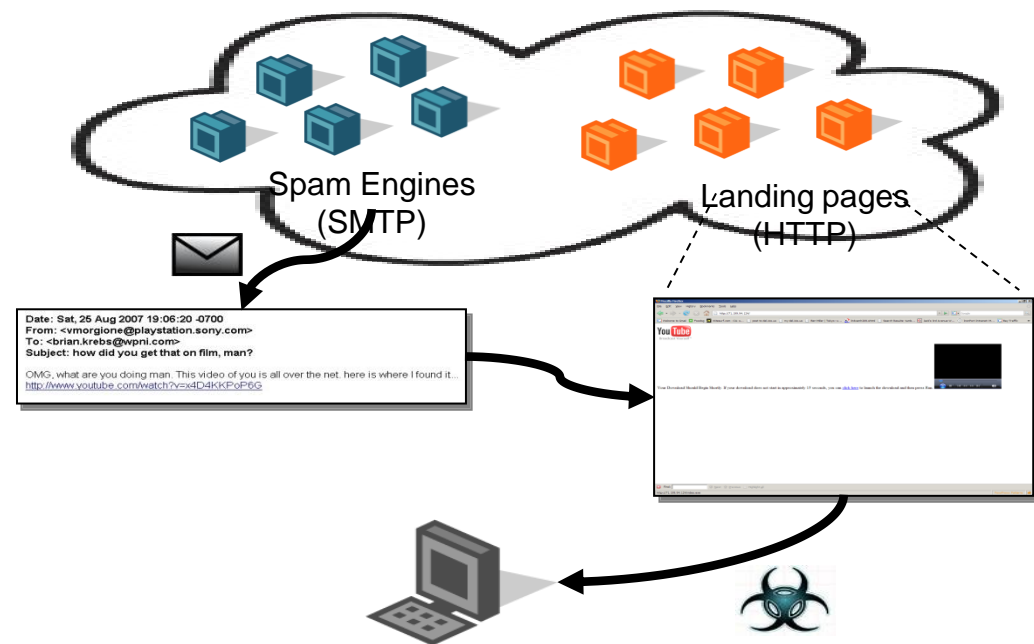
1000 contaminated PC in the USA \$110

Rented per hour, with phone support available

- **Self-expanding:** Recruiting emails & Spam

- **Coordinated:** Synchronizes email spam with web landing pages

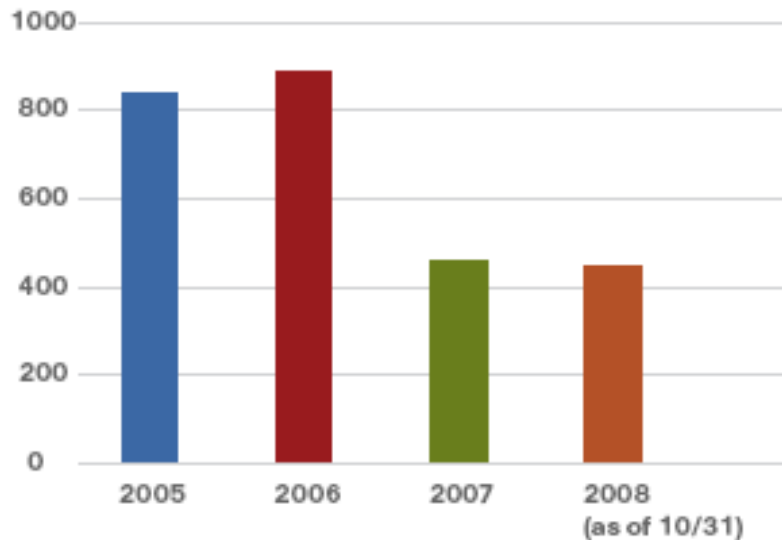
- **Peer-to-Peer:** Uses P2P network to communicate



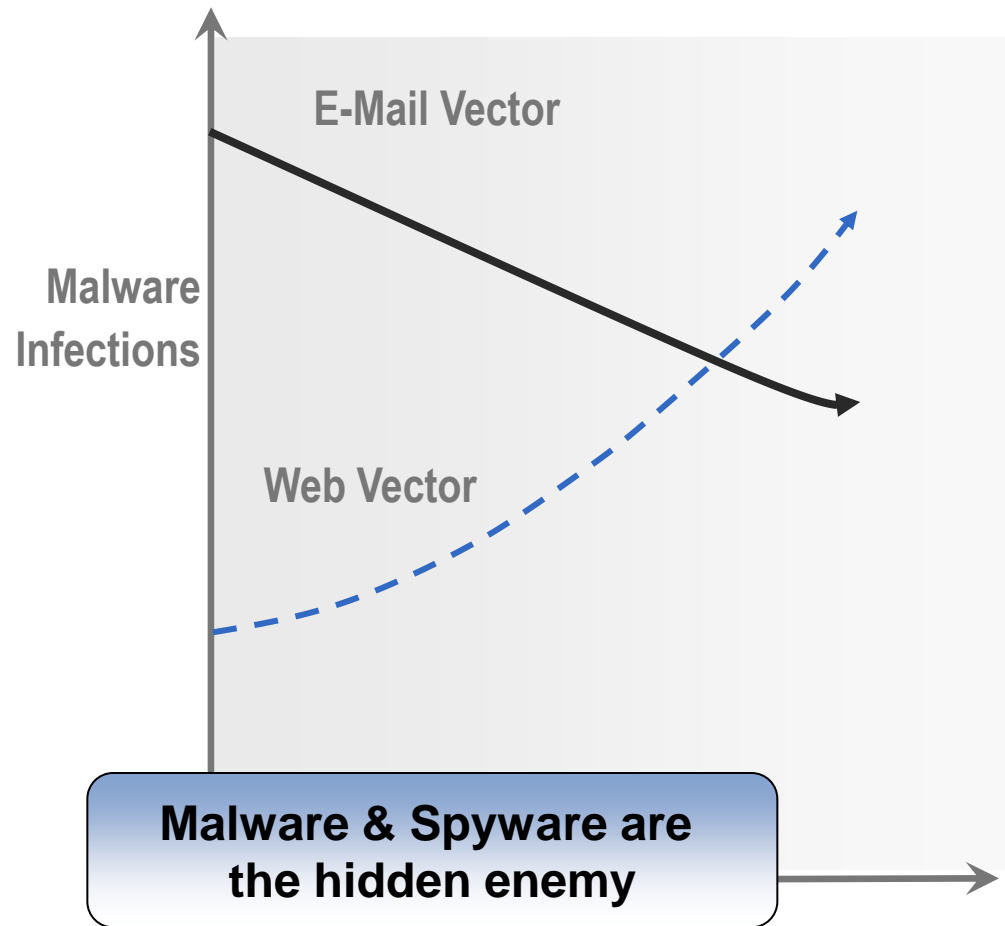
**2007** : Storm is born

**2008** : Storm still active, joined by Kraken/Bobax & Asprox

# Threat vectors are changing



Volume of Malware Successfully Propagated via Email Attachments



# Legitimate Sites Hacked

- Over **87%** of all Web-based **threats today** are using **exploited web sites\***
- **9 out of 10** web sites vulnerable to attack\*\*
- A commonly used technique today: iFrame attacks
  1. A legitimate site is hacked (iFrame added on a page)
  2. The user is re-directed by the iFrame towards an infected website
  3. A malware is automatically downloaded on the desktop by exploiting a vulnerability of the web browser
- **Cannot be secured with legacy URL filtering solutions**



\*Source: Cisco TOC

\*\*Source: White Hat Security, Website Sec Statistics Report 10/2007

# What is one of the first things you teach your children?



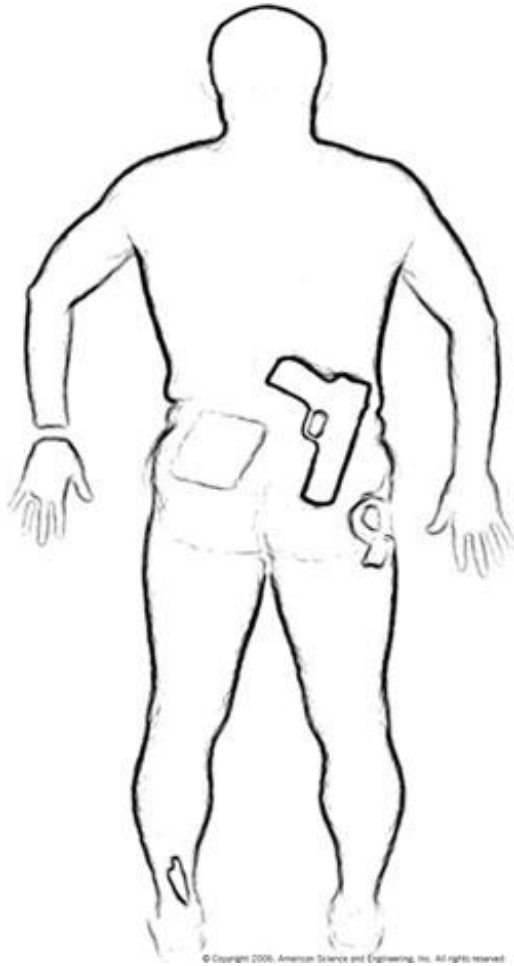
# Would you let him in?



# And her?



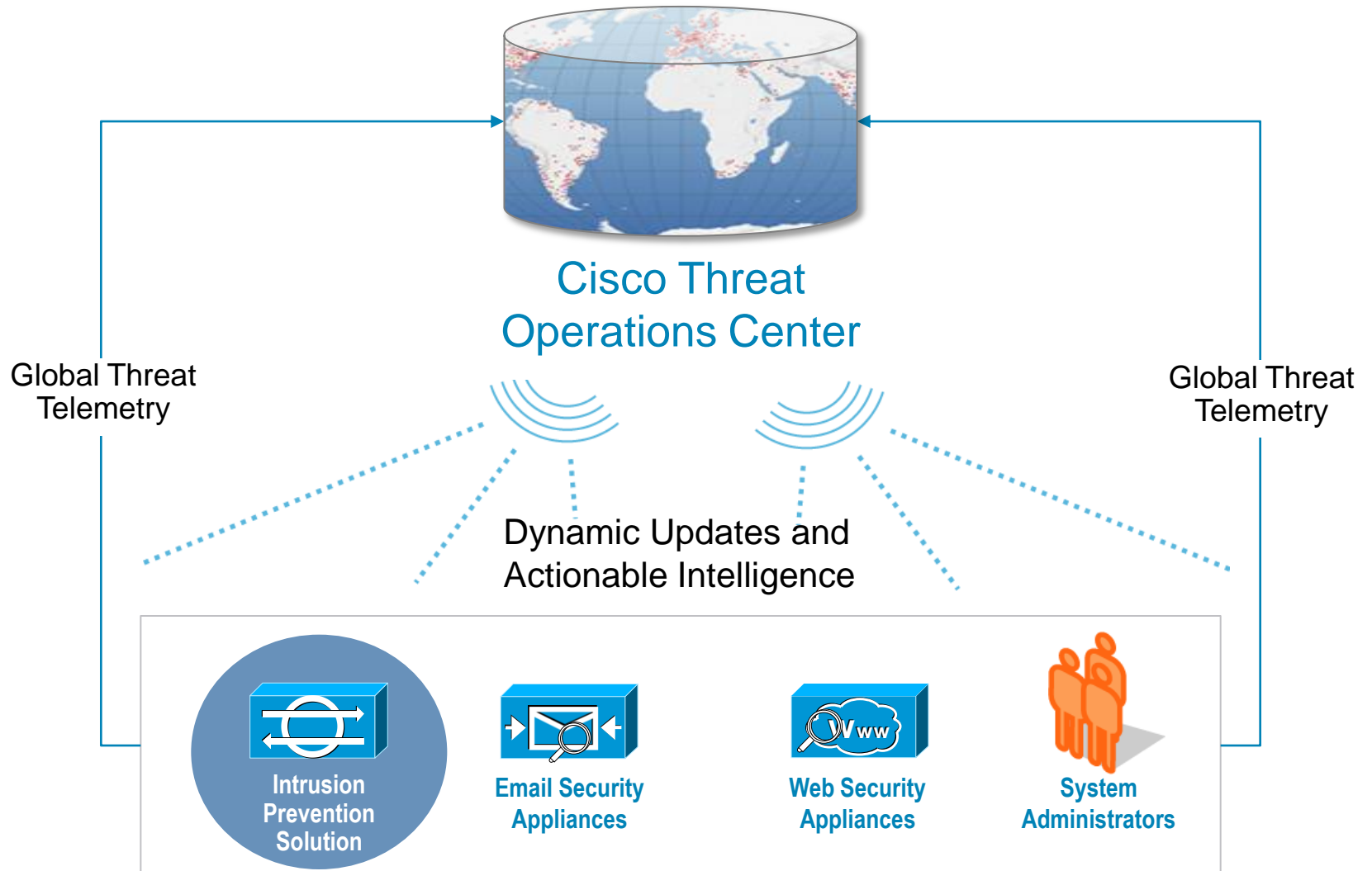
# To search for specific content?



© Copyright 2006, American Science and Engineering, Inc. All rights reserved.



# Cisco Global Threat Correlation



# Cisco IronPort SensorBase®



- Statistics on more than 30% of the world's e-mail traffic
- New threats & alerts detection
- More than **150 parameters** to build reputation scores

- Data Volume
- Message Structure
- Complaints
- Blacklists, whitelists
- Off-line data

## E-Mail Reputation Filters



Reputation Score

- URL blacklists & whitelists
- HTML Content
- Domain Info
- Known "bad" URLs
- Website history...

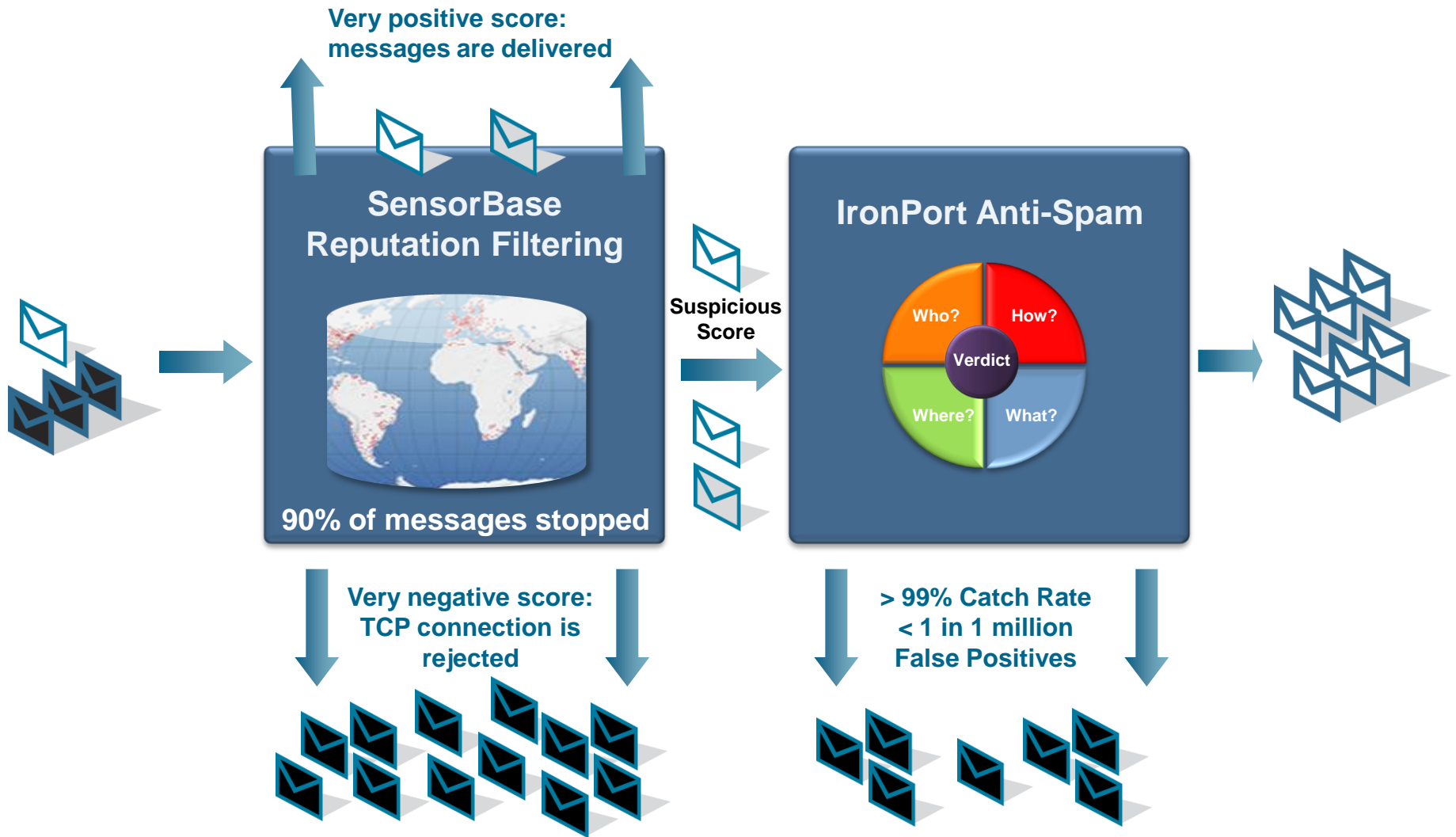
## Web Reputation Filters



Reputation Score

# E-Mail Reputation

*90% of messages stopped at connection level*

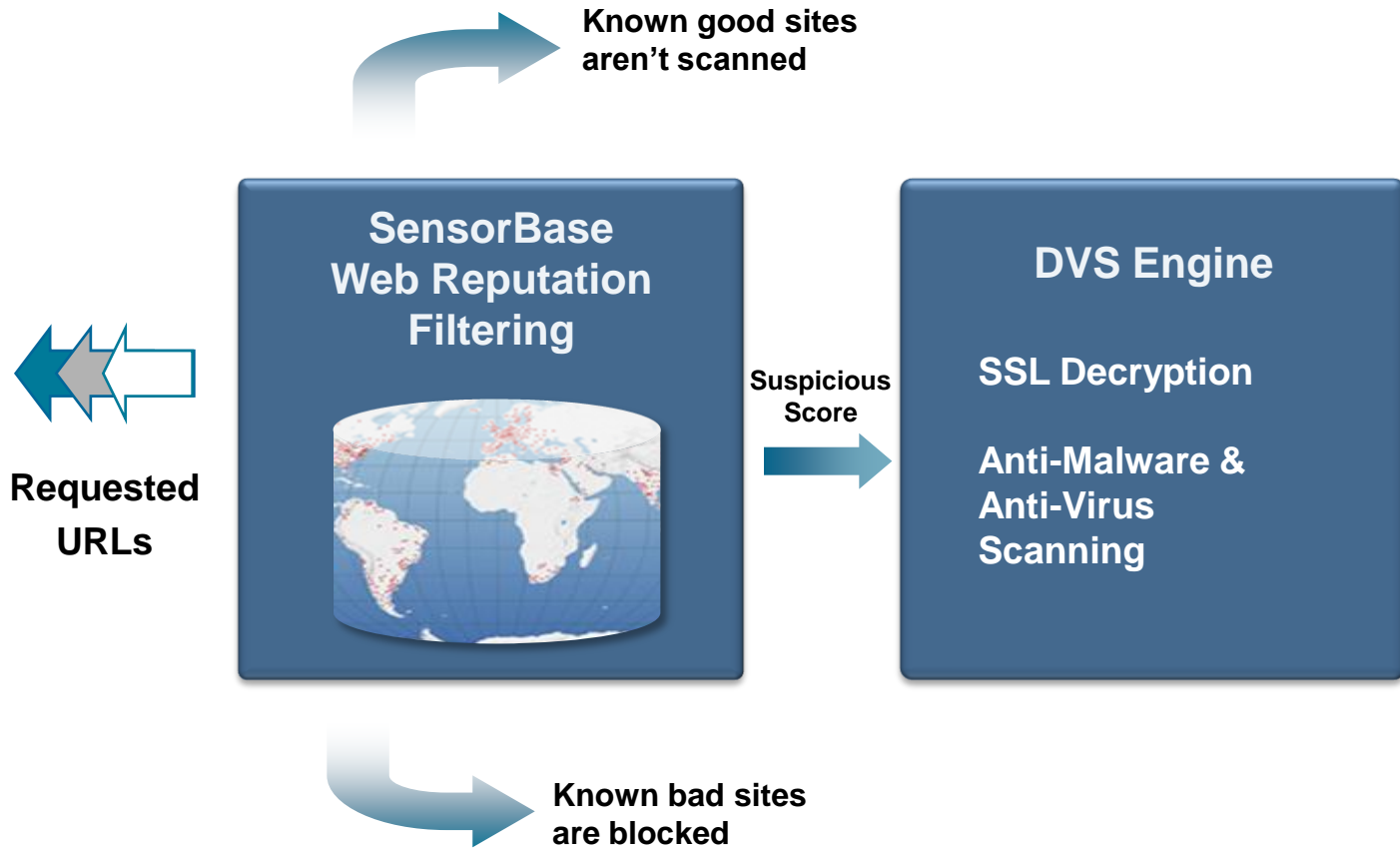


# SenderBase Reputation Filtering

## The Cisco Example

Message Category	%	Messages
<b>Stopped by Reputation Filtering</b>	<b>93.1%</b>	<b>700,876,217</b>
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
<b>Total Threat Messages:</b>	<b>96.8%</b>	<b>728,797,126</b>
Clean Messages	3.2%	24,102,874
<b>Total Attempted Messages:</b>		<b>752,900,000</b>

# Web Reputation Filtering





THE INDUSTRY-LEADING  
CISCO IRONPORT C650  
EMAIL SECURITY APPLIANCE

**TRY BEFORE YOU BUY**

Sign up today to  
evaluate the  
Cisco IronPort email  
security solution  
**FREE.**

  
CISCO

© 2009 Cisco Systems, Inc.

95% of companies  
who try Cisco IronPort  
become customers.

*Contact:*

[scommero@cisco.com](mailto:scommero@cisco.com)



**CISCO**