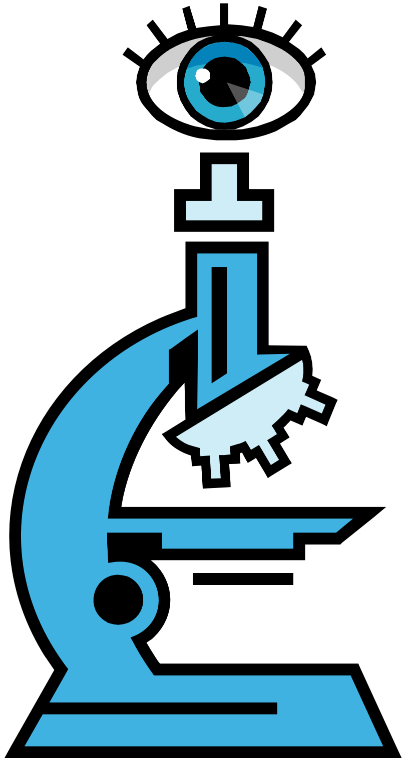
Cisco Security Intelligence Operations (Cisco SIO) Overview

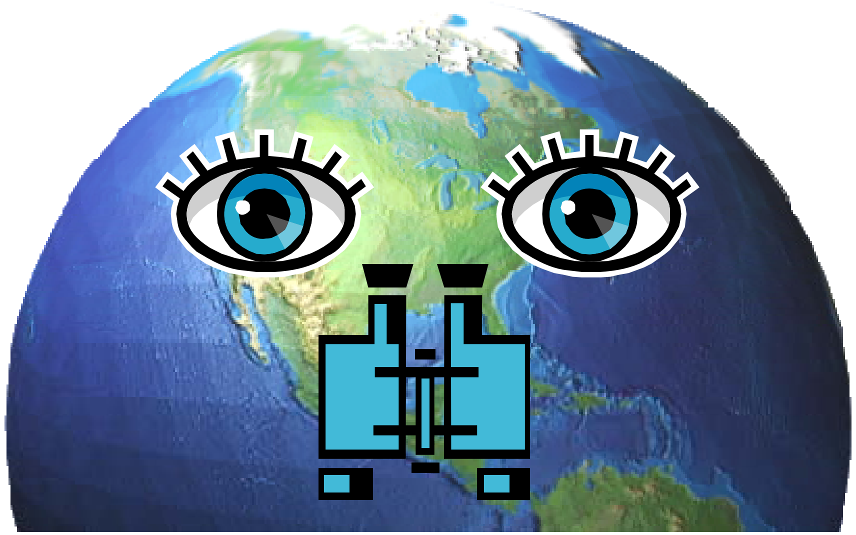
Karaked Kedchumpol
System Engineer

A Seismic Shift

- **2000-2008:** IT security products look deeper



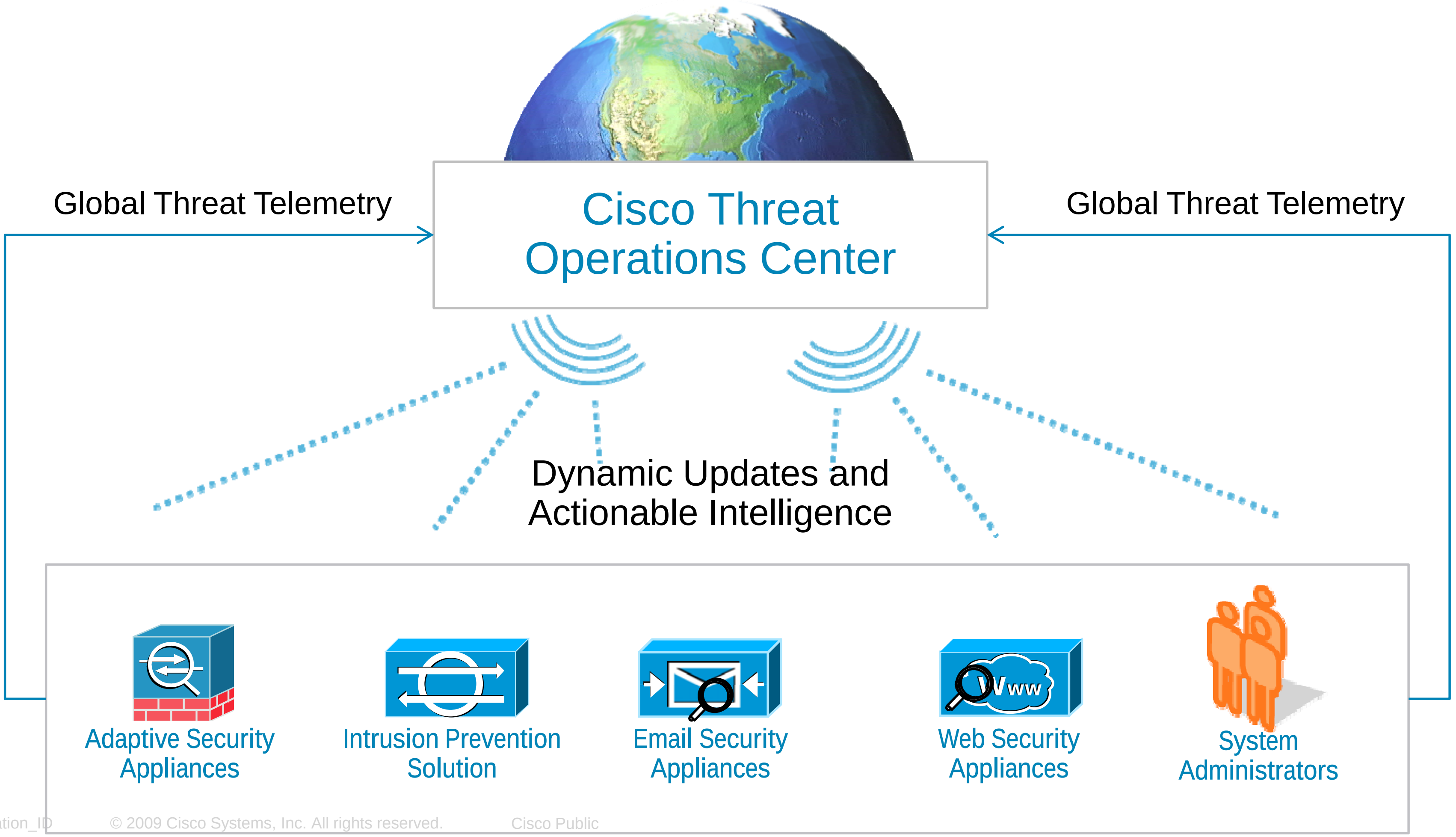
- **2009:** Cisco Security products look around, respond faster



Cisco Security Intelligence Operations (SIO)

Overview

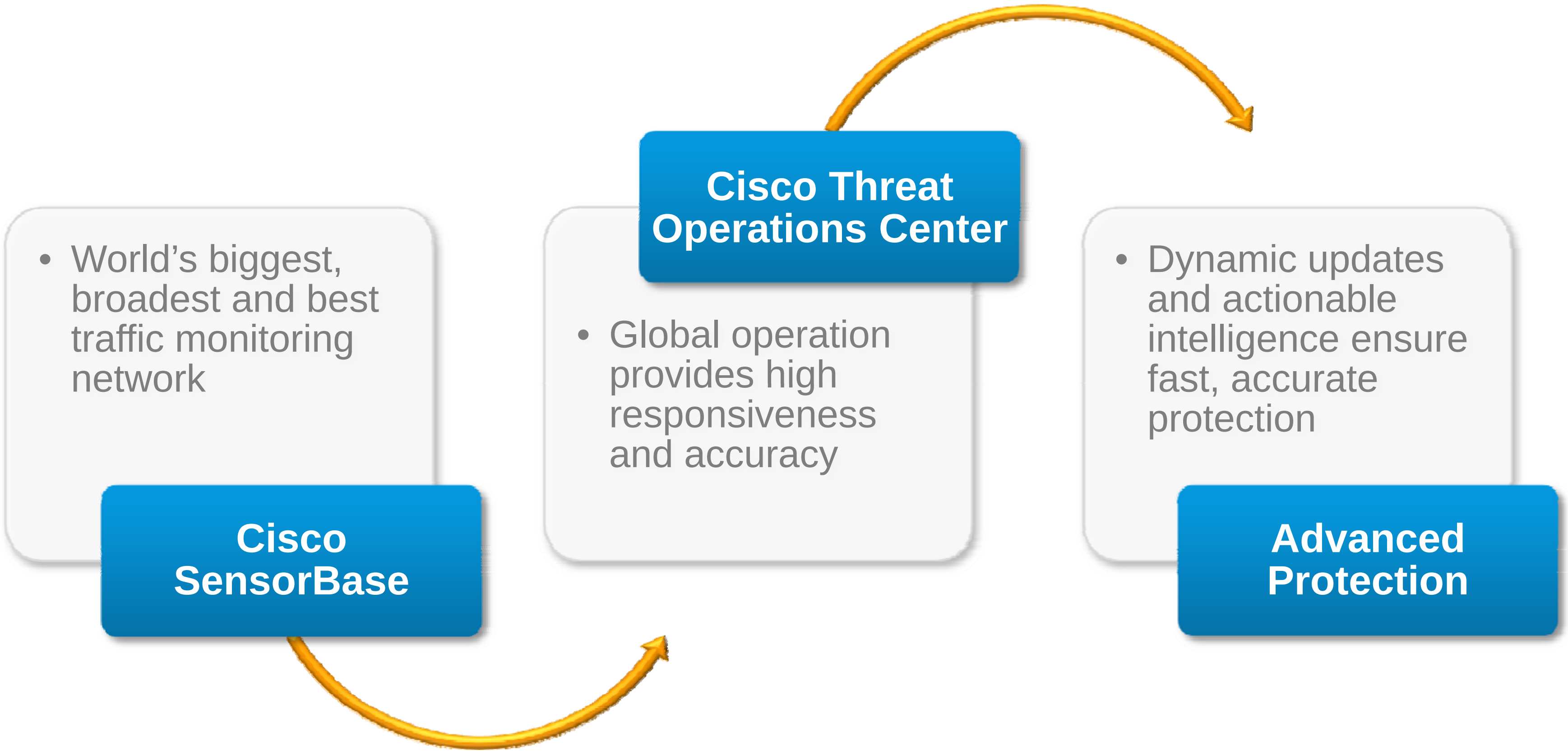
Most Accurate Protection Against a Broad Range of Threats


Global Threat Telemetry
Cisco Threat Operations Center
Global Threat Telemetry
Dynamic Updates and Actionable Intelligence
Adaptive Security Appliances
Intrusion Prevention Solution
Email Security Appliances
Web Security Appliances
System Administrators

Cisco SIO

Key Components

Powerful Ecosystem Enables Fast, Accurate Protection



Cisco SensorBase

- World's biggest, broadest and best traffic monitoring network

Cisco Threat Operations Center

- Global operation provides high responsiveness and accuracy

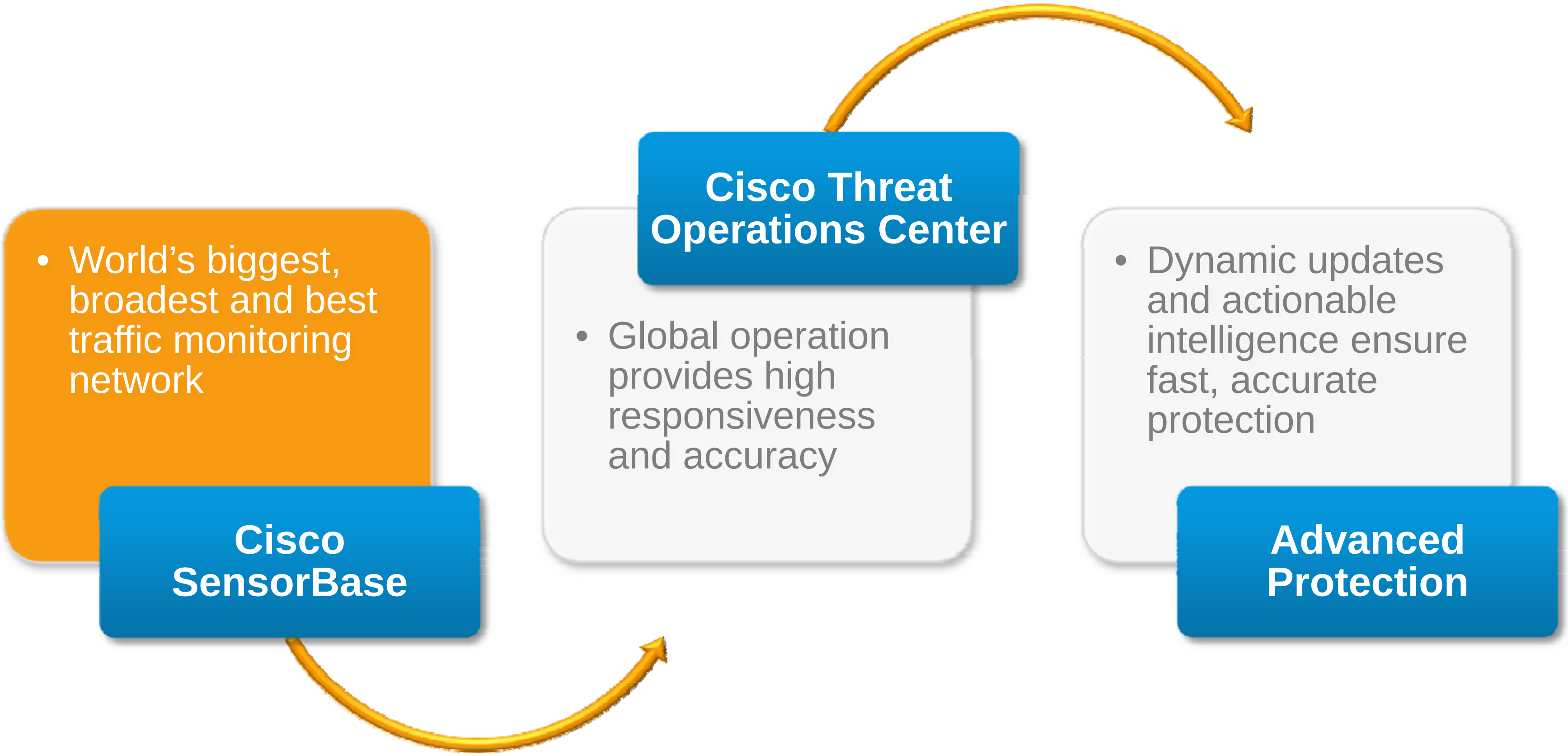
Advanced Protection

- Dynamic updates and actionable intelligence ensure fast, accurate protection

Cisco SIO

Cisco SensorBase

Largest Network, Highest Data Quality, Unmatched Breadth



- World's biggest, broadest and best traffic monitoring network

Cisco SensorBase

Cisco Threat Operations Center

- Global operation provides high responsiveness and accuracy

- Dynamic updates and actionable intelligence ensure fast, accurate protection

Advanced Protection

Cisco SensorBase Network

Unmatched Visibility Into Global Threats

Most Devices

1M security devices, 10M clients shipped per year

Core Internet routers

Cloud-based services

Largest Footprint

30% of the world’s email traffic

200+ parameters

368GB per day sensor feeds

Diverse Sources

Eight of the top ten ISPs

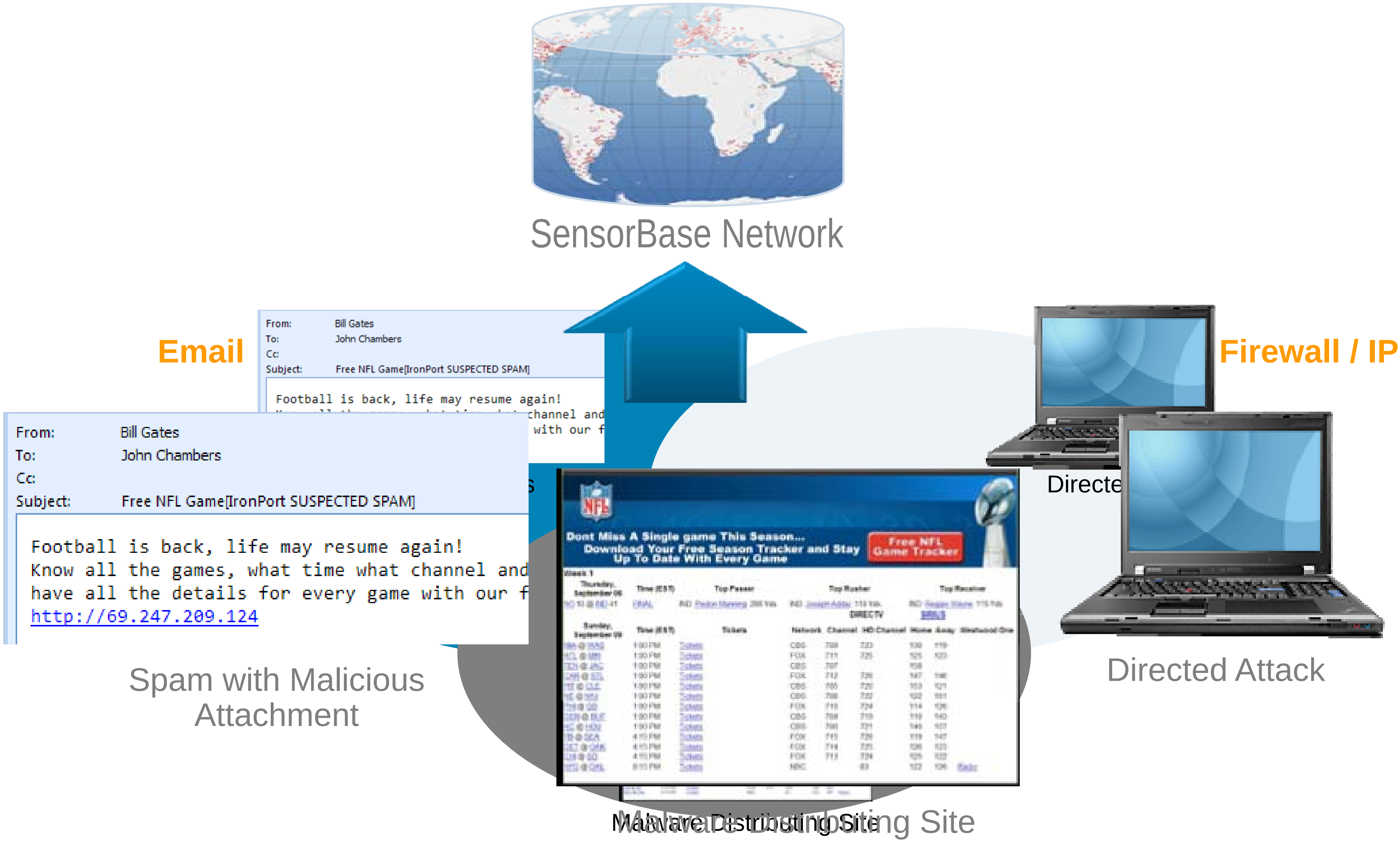
Fortune 500, Global 2000, universities, SMBs

152 third-party feeds

First to Combine Network and Application Layer Data

Cisco SensorBase Network

Unmatched Breadth


SensorBase Network
Email
Firewall / IPS
Directe
Dont Miss A Single game This Season...
Download Your Free Season Tracker and Stay
Up To Date With Every Game
Free NFL Game Tracker
Malware Distributing Site

From: Bill Gates
To: John Chambers
Cc:
Subject: Free NFL Game[IronPort SUSPECTED SPAM]

Football is back, life may resume again!

From: Bill Gates
To: John Chambers
Cc:
Subject: Free NFL Game[IronPort SUSPECTED SPAM]

Football is back, life may resume again!
Know all the games, what time what channel and
have all the details for every game with our f
http://69.247.209.124

Spam with Malicious Attachment

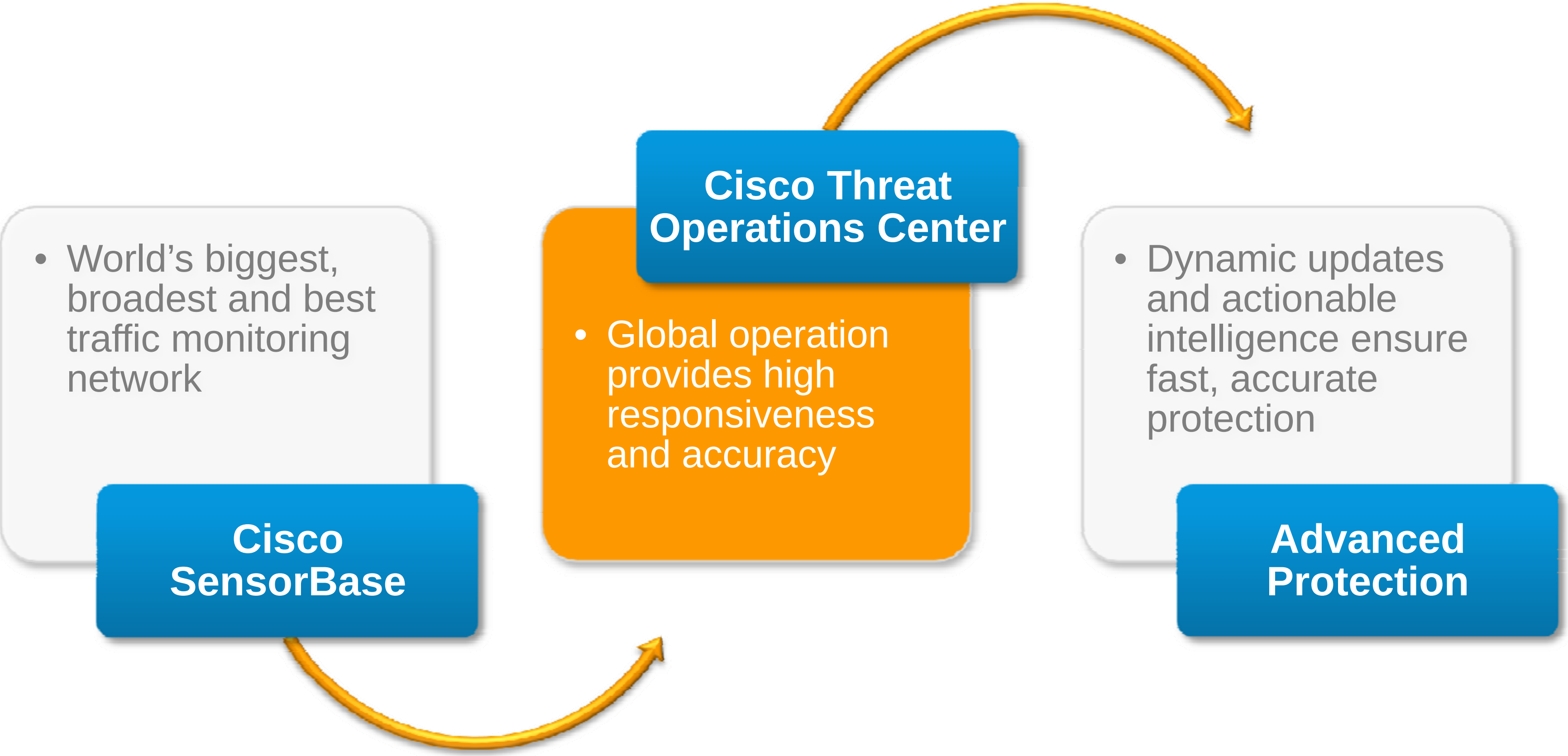
Malware Distributing Site

Directed Attack

Cisco SIO

Cisco Threat Operations Center (TOC)

Advanced Research and Development, Security Modeling, Experienced Analysts



- World's biggest, broadest and best traffic monitoring network

Cisco SensorBase

Cisco Threat Operations Center

- Global operation provides high responsiveness and accuracy

- Dynamic updates and actionable intelligence ensure fast, accurate protection

Advanced Protection

Cisco Threat Operation Center

Advanced Research and Development

- **Millions in R&D investment**

  Threat experts and statisticians

  Equipment and infrastructure

  Thought leadership, prevention and best practices expertise

  76 patents

- **Innovative services**

  IPS Global Correlation

  ASA Botnet Traffic Filters

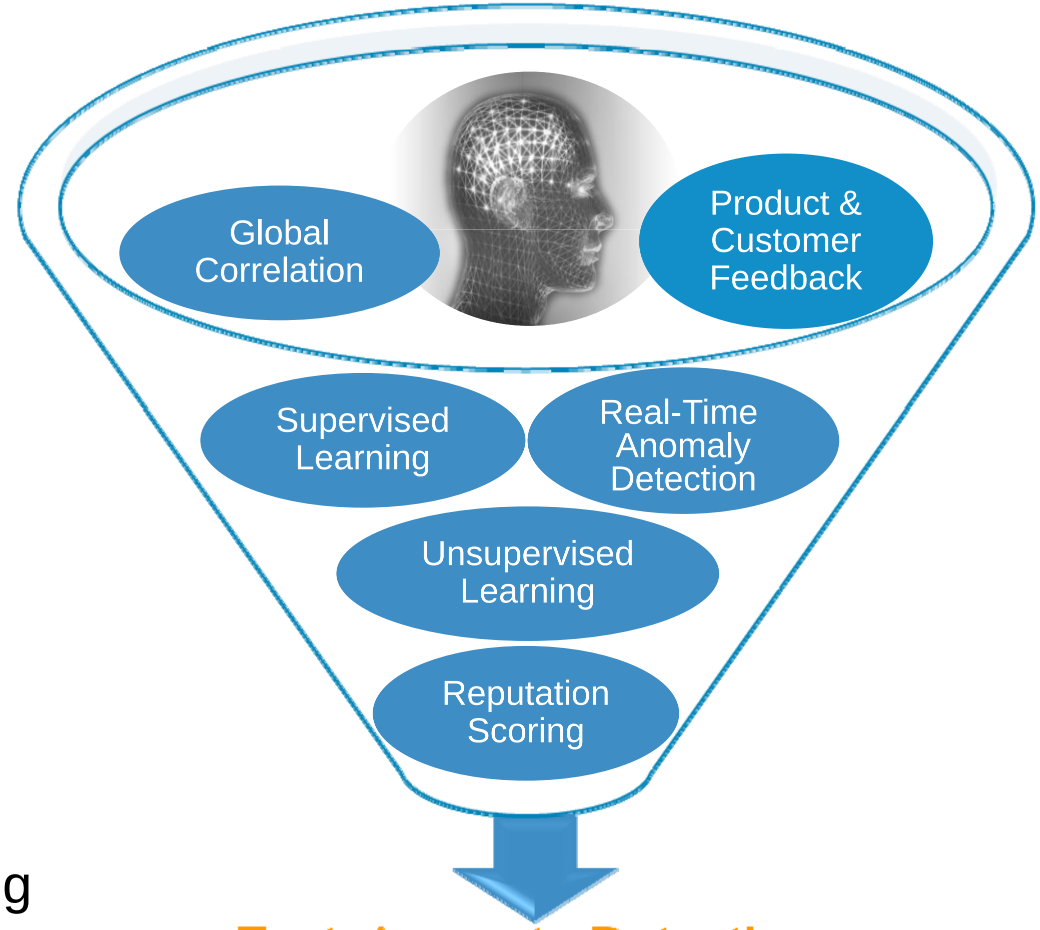
  Virus Outbreak Filters

  Reputation Filters (IPS, email, web, etc.)

Cisco Threat Operations Center

Sophisticated Security Modeling and Remediation

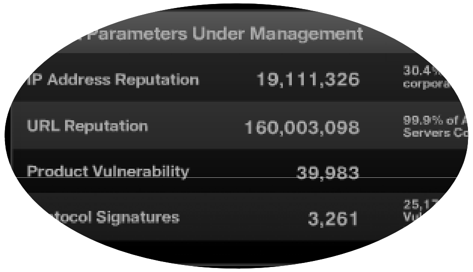
- **Advanced algorithms**
  - Dynamic real-time scoring
  - Fast threat identification
  - Automated rule and/or signature creation
  - Human-aided rule creation
- **White Hat engineers**
  - Penetration testing
  - Botnet infiltration
  - Malware reverse engineering



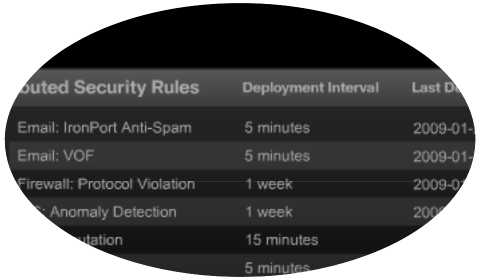
Fast, Accurate Detection, Advanced Mitigations

Cisco Threat Operations Center

Ensuring Accuracy and Responsiveness



Parameters Under Management		
IP Address Reputation	19,111,326	30.4% corpora
URL Reputation	160,003,098	99.9% of A Servers Co
Product Vulnerability	39,983	
tocol Signatures	3,261	25,17 Vu



buted Security Rules	Deployment Interval	Last D
Email: IronPort Anti-Spam	5 minutes	2009-01-
Email: VOF	5 minutes	2009-01-
Firewall: Protocol Violation	1 week	2009-0
: Anomaly Detection	1 week	200
utation	15 minutes	
	5 minutes	

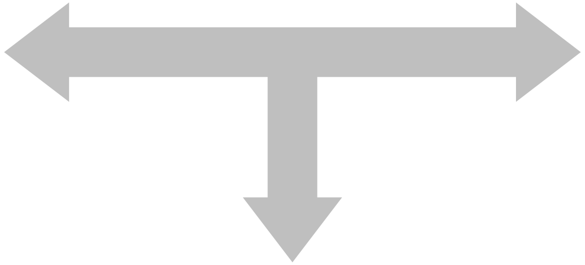
Experienced Analysts

500 analysts

European and Asian languages

1 Cisco Fellow

80+ Ph.D.s, CCIEs, CISSPs, MSCEs



24x7x365 Operations

5 threat operations center locations around the globe

San Jose, San Bruno, Austin, North Carolina, Shanghai

Powerful Tools

Dynamic updates

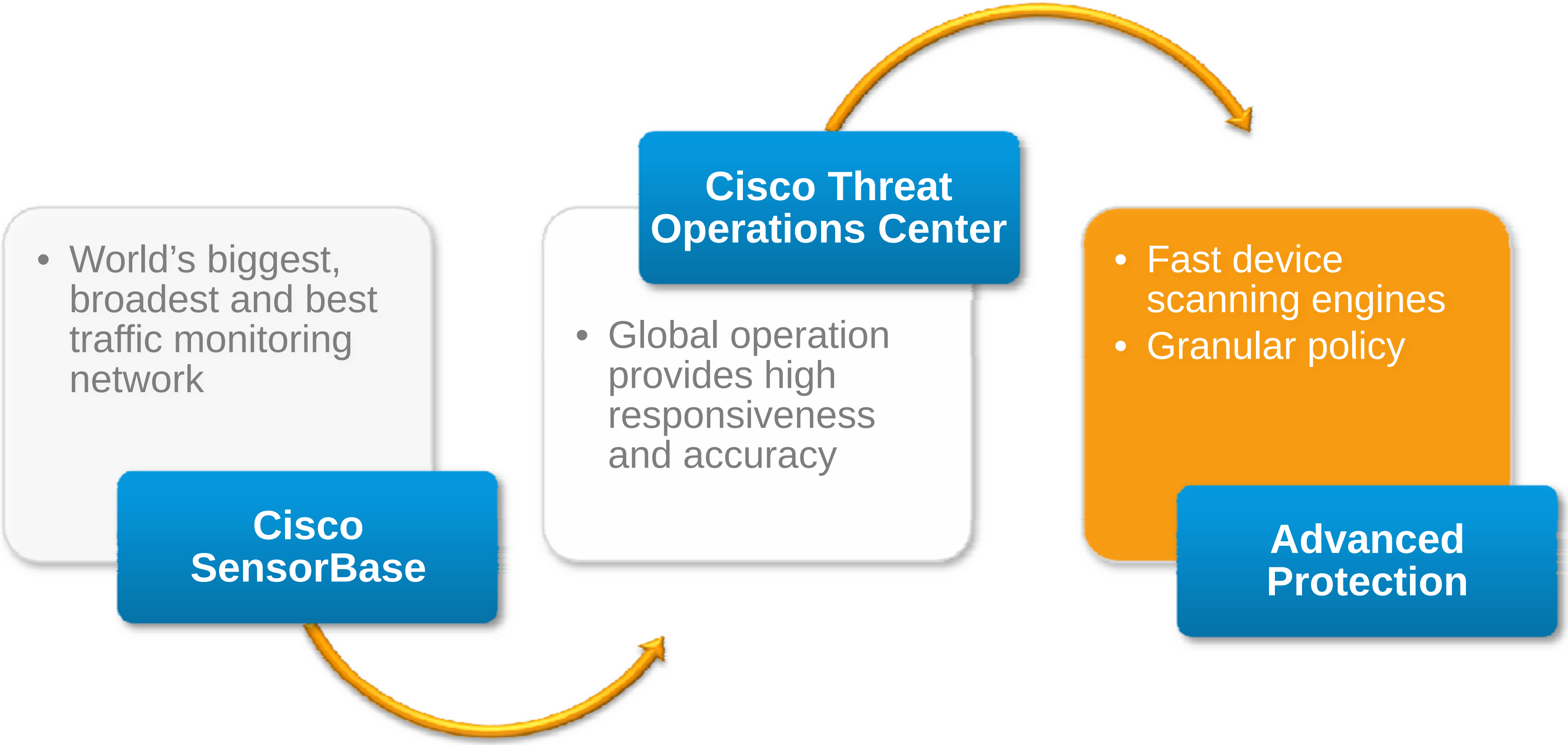
Correlation and data mining

Advanced rule approval, creation and publishing applications

Cisco SIO

Broadest Enforcement Capabilities

Fast Device Scanning Engines and Granular Policy



- World's biggest, broadest and best traffic monitoring network

Cisco SensorBase

Cisco Threat Operations Center

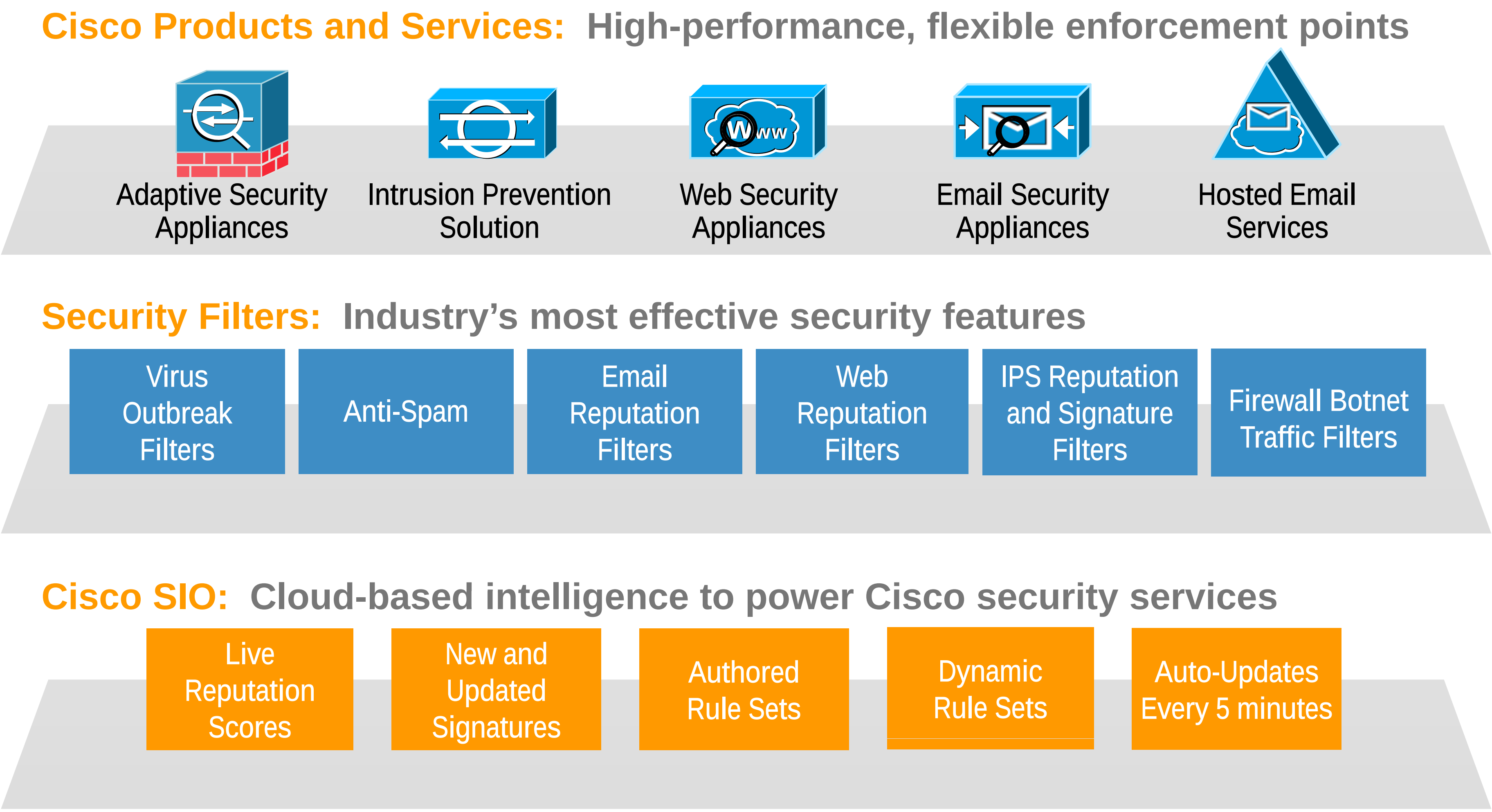
- Global operation provides high responsiveness and accuracy

- Fast device scanning engines
- Granular policy

Advanced Protection

Advanced Protection

Putting It All Together



Cisco Products and Services: **High-performance, flexible enforcement points**

- Adaptive Security Appliances
- Intrusion Prevention Solution
- Web Security Appliances
- Email Security Appliances
- Hosted Email Services

Security Filters: **Industry’s most effective security features**

- Virus Outbreak Filters
- Anti-Spam
- Email Reputation Filters
- Web Reputation Filters
- IPS Reputation and Signature Filters
- Firewall Botnet Traffic Filters

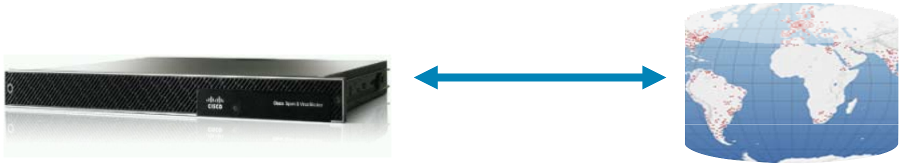
Cisco SIO: **Cloud-based intelligence to power Cisco security services**

- Live Reputation Scores
- New and Updated Signatures
- Authored Rule Sets
- Dynamic Rule Sets
- Auto-Updates Every 5 minutes

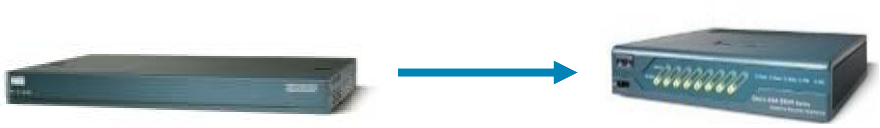
Cisco SIO

Works Three Ways

- Devices contribute to Cisco SIO, and receive rules and reputation data

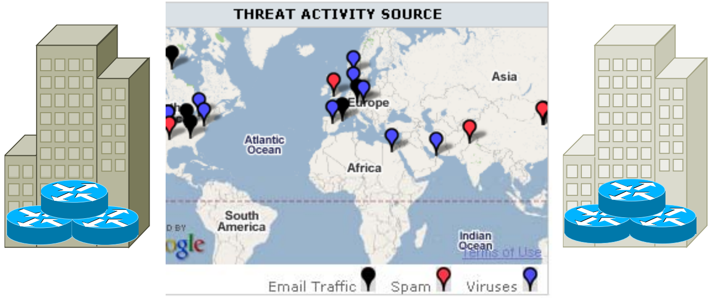


- Devices may trigger rule and configuration changes in other local devices



FUTURE: *Devices may redirect traffic to other devices for further scanning*

- Security events in one Cisco protected network indirectly trigger rules in other networks

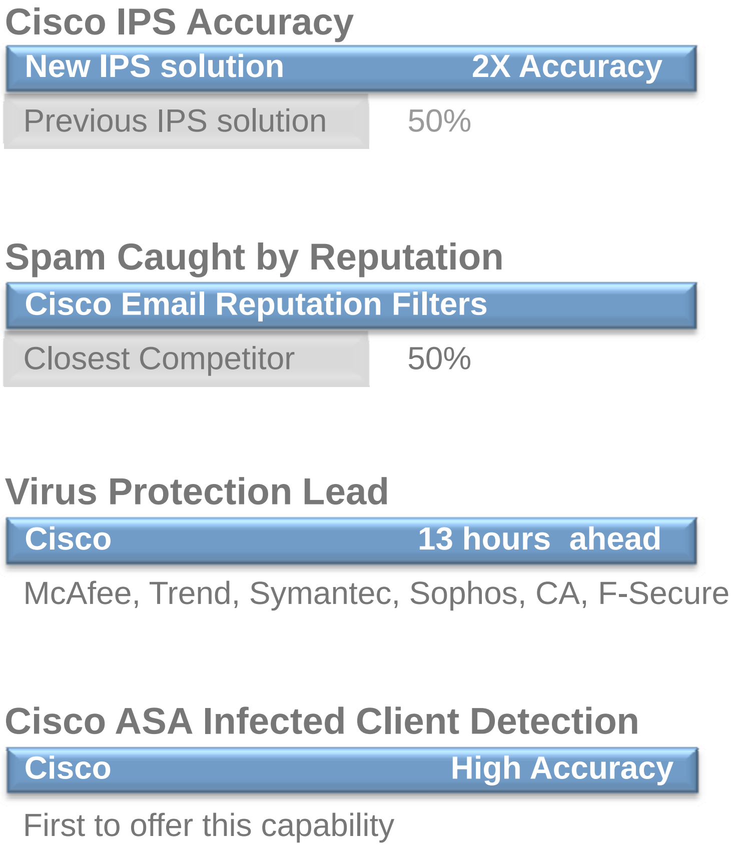


Cisco SIO Effectiveness

Leading Accuracy and Responsiveness

- Cisco detects and acts against unwanted traffic faster and more accurately than any other vendor

- Other companies lack the human, network and device-level intelligence that makes Cisco SIO so effective



Cisco IPS Accuracy

New IPS solution 2X Accuracy

Previous IPS solution 50%

Spam Caught by Reputation

Cisco Email Reputation Filters

Closest Competitor 50%

Virus Protection Lead

Cisco 13 hours ahead

McAfee, Trend, Symantec, Sophos, CA, F-Secure

Cisco ASA Infected Client Detection

Cisco High Accuracy

First to offer this capability

Global Correlation In Action

Network IPS to Global IPS

08:00 GMT

- A sensor in Australia detects new malware
- A sensor in Russia detects a botnet issuing new commands
- A sensor in Korea detects a virus mutating
- A sensor in Florida detects a hacker probing major financial institutions

08:15 GMT

- **All Cisco IPS customers protected**

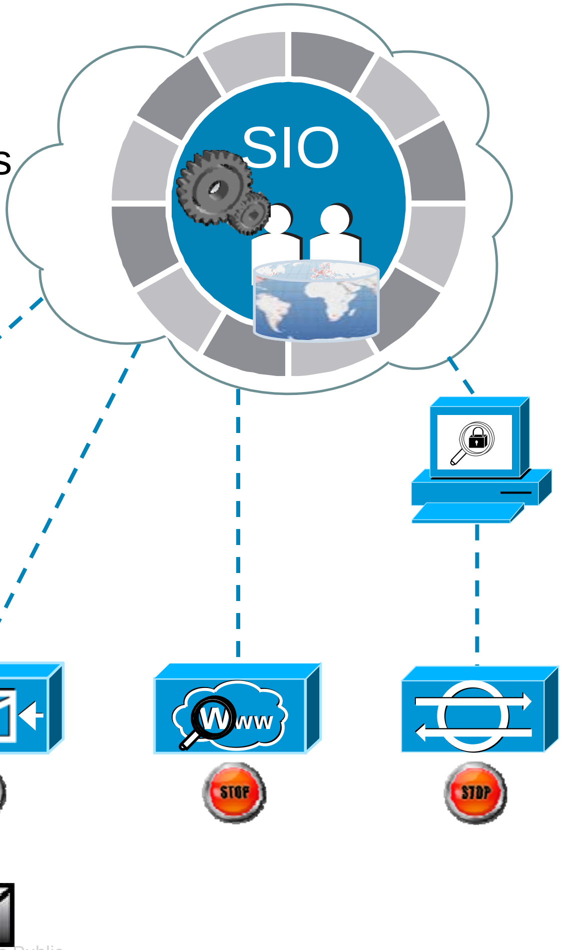
Fast, Complete and Accurate Protection Using Global IPS Data

Cisco IPS has **twice** the IPS deployment of the next vendor, collecting billions of data points worldwide

Cisco SIO In Action

Obama Botnet

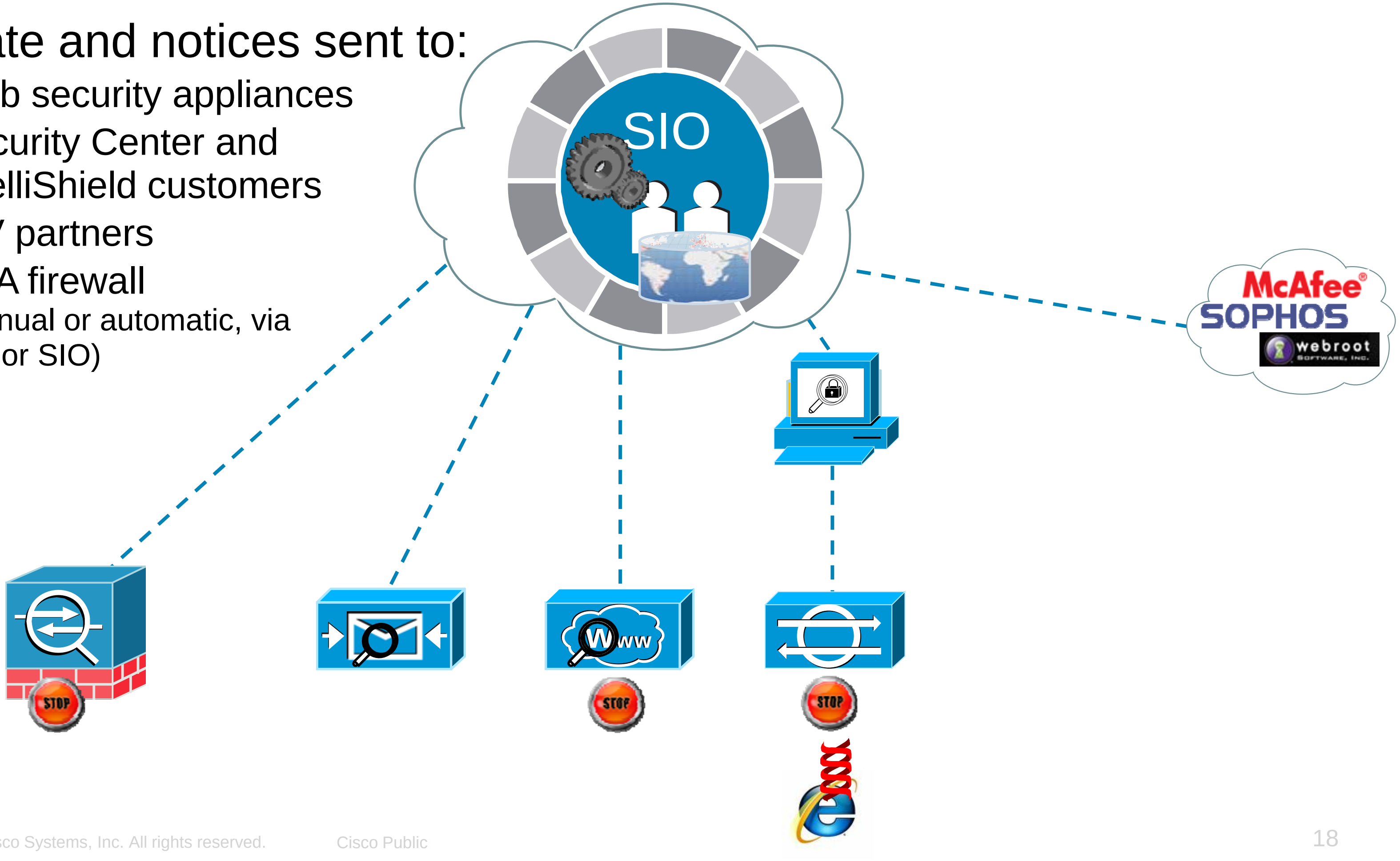
1. Baseline threat data installed in Cisco security devices
2. Spoofed email for Obama speech triggers alert to Cisco SIO
3. Rule update to:
   - ASA firewall
   - Web security appliances
   - IPS
4. Botnet servers blocked



Cisco SIO In Action

Internet Explorer Browser Vulnerability

1. IPS senses anomaly, alerts MARS, escalates to SIO researchers
2. TOC finds new botnet command and control hosts, modifies rules
3. Update and notices sent to:
   - Web security appliances
   - Security Center and IntelliShield customers
   - ISV partners
   - ASA firewall
     (manual or automatic, via IPS or SIO)



Cisco Security Intelligence Operations

Vision

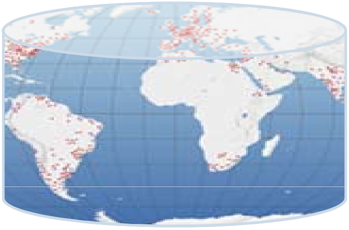
- More Cisco devices will be linked into the Cisco Shared Defense Network
- This will provide global analysis, and be more informative about how your Cisco network is defending itself

Global Correlation

Cisco Global Correlation

SensorBase: World's Largest Traffic Monitoring Network

LARGEST FOOTPRINT | GREATEST BREADTH | FULL CONTEXT ANALYSIS



Cisco SensorBase

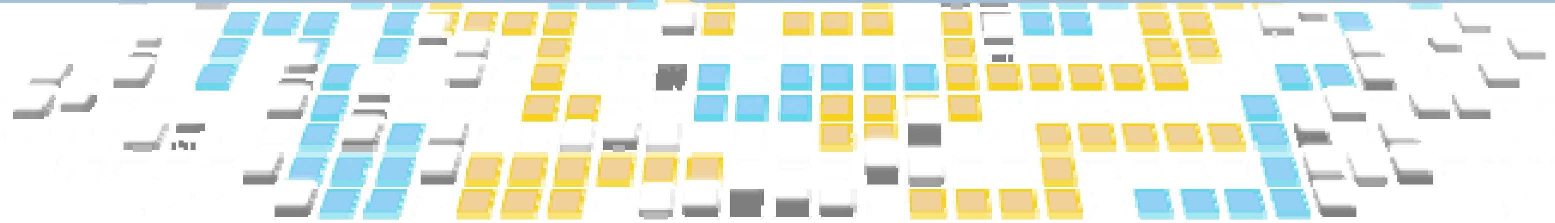
700,000+ sensors deployed globally

8 of the top 10 global ISPs

Over 500GB of data per day

152 third party feeds

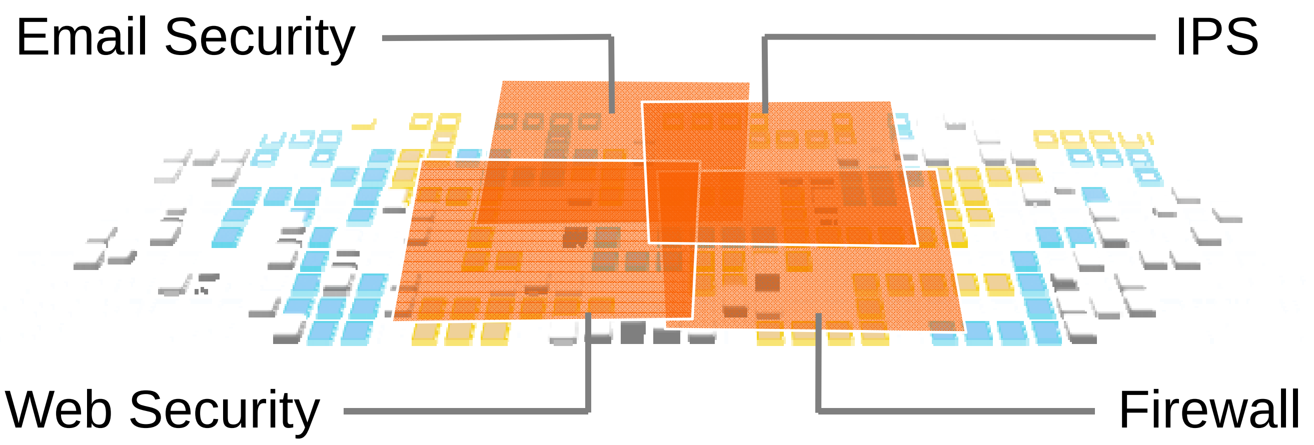
Over 30% of the world's email traffic



Cisco Global Correlation

Unmatched Breadth

LARGEST FOOTPRINT | **GREATEST BREADTH** | FULL CONTEXT ANALYSIS

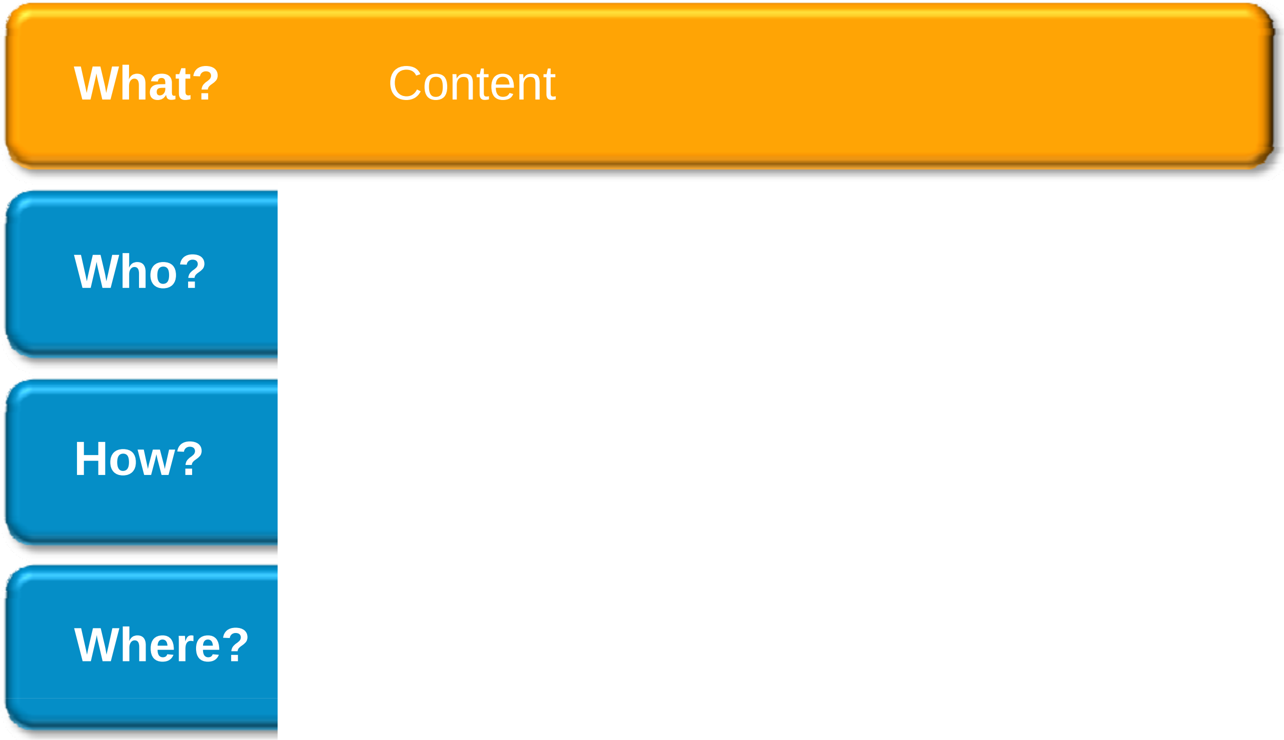


Identifying a global botnet requires complete visibility across all threat vectors

Global Correlation

Full Context Analysis: Seeing the Whole Picture

LARGEST FOOTPRINT | GREATEST BREADTH | **FULL CONTEXT ANALYSIS**



Cisco IPS 7.0

Network IPS to Global IPS

- **Coverage**

  Twice the effectiveness of signature-only IPS

- **Accuracy**

  Reputation analysis decreases false positives

- **Timeliness**

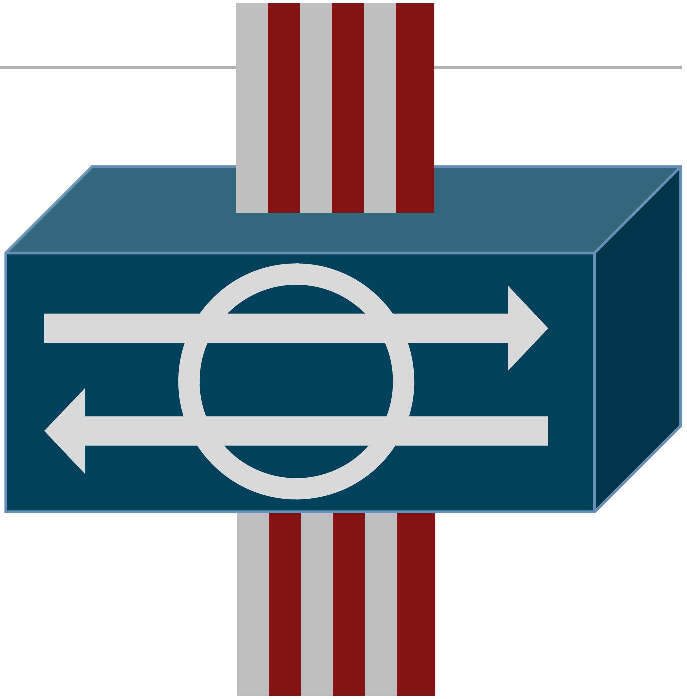
  100x faster than traditional signature-only methods

IPS Reputation Filtering powered by Global Correlation

Defeating SQL Injection

The Challenge of Traditional Signature-Based IPS

	What SIGNATURES Find	*Verdict: UNKNOWN*
What?	*SQL Command Fragments in Web Traffic*	

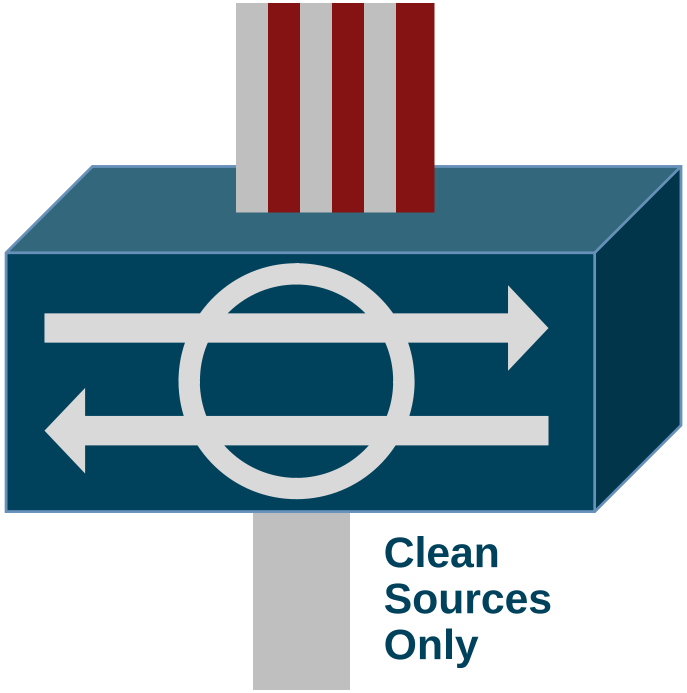


IPS Reputation Enables Protection

Powered By Global Correlation

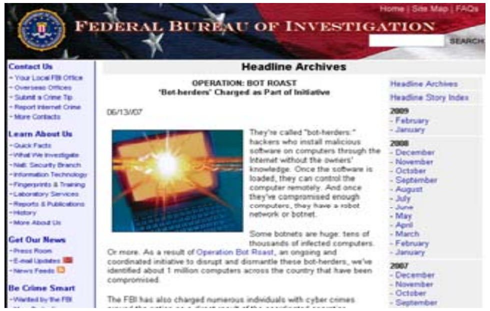
	What CISCO IPS Finds
What?	*SQL Command Fragments in Web Traffic*
How?	*First HTTP connection*
Who?	*Dynamic IP Address* *Dynamic DNS* *History of Web Attacks*
Where?	*Within Heavily Compromised* *.Asia Network* *History of Botnet Activity*

Verdict: BLOCK



ASA Botnet traffic Filter

Botnet Epidemic



Headline Archives

OPERATION: BOT ROAST
'Bot-herders' Charged as Part of Initiative

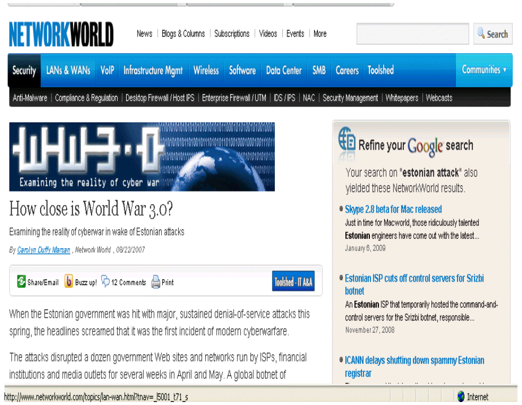
06/13/07

They're called "bot-herders:" hackers who install malicious software on computers through the Internet without the owners' knowledge. Once the software is loaded, they can control the computer remotely. And once they've compromised enough computers, they have a robot network or botnet.

Some botnets are huge: tens of thousands of infected computers. Or more. As a result of Operation Bot Roast, an ongoing and coordinated initiative to disrupt and dismantle these bot-herders, we've identified about 1 million computers across the country that have been compromised.

The FBI has also charged numerous individuals with cyber crimes

"Operation BotRoast"
—FBI


NETWORKWORLD
News | Blogs & Columns | Subscriptions | Videos | Events | More
Search
Security
LANs & WANs
VoIP
Infrastructure Mgmt
Wireless
Software
Data Center
SMB
Careers
Toolshed
Communities
Anti-Malware | Compliance & Regulation | Desktop Firewall / Host IPS | Enterprise Firewall / UTM | IDS / IPS | NAC | Security Management | Whitepapers | Webcasts
WW3.0
Examining the reality of cyber war
Share/Email
Buzz up!
12 Comments
Print
Toolshed - IT A&A
Refine your Google search
Internet

How close is World War 3.0?

Examining the reality of cyberwar in wake of Estonian attacks

By Carolyn Duffy Marsan , Network World , 08/22/2007

When the Estonian government was hit with major, sustained denial-of-service attacks this spring, the headlines screamed that it was the first incident of modern cyberwarfare.

The attacks disrupted a dozen government Web sites and networks run by ISPs, financial institutions and media outlets for several weeks in April and May. A global botnet of

Your search on "estonian attack" also yielded these NetworkWorld results.

- Skype 2.8 beta for Mac released
  Just in time for Macworld, those ridiculously talented Estonian engineers have come out with the latest...
  January 6, 2009
- Estonian ISP cuts off control servers for Srizbi botnet
  An Estonian ISP that temporarily hosted the command-and-control servers for the Srizbi botnet, responsible...
  November 27, 2008
- ICANN delays shutting down spammy Estonian registrar

http://www.networkworld.com/topics/lan-wan.html?tnav=_l5001_t71_s

"How Close Is World War 3.0?" —Network World

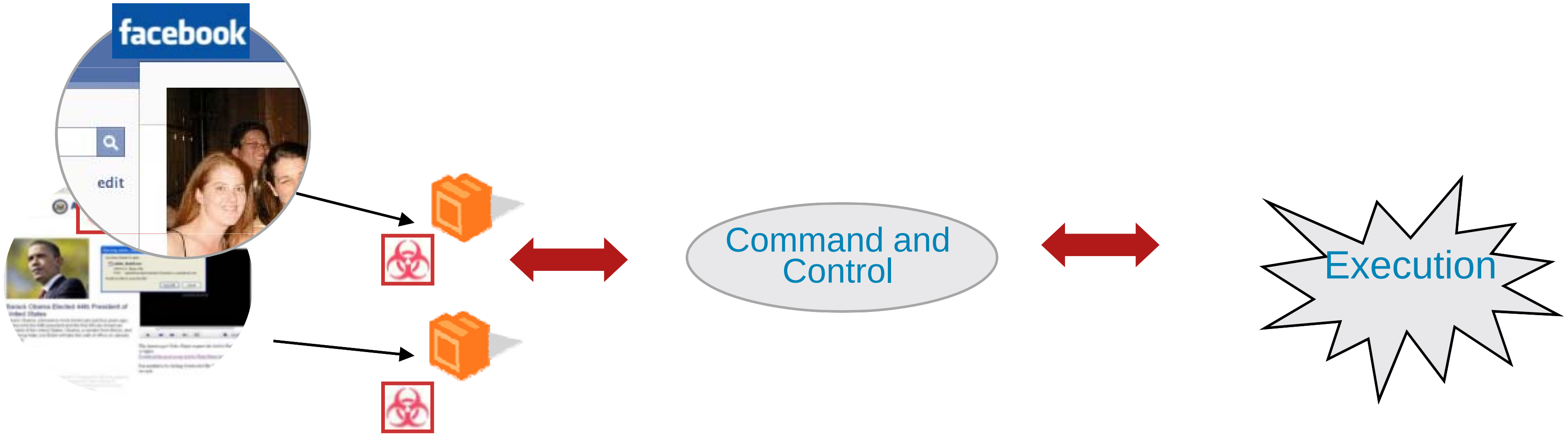
Overview

- Botnets = network of compromised computers
- 1 to 5 million hosts are believed to have been compromised in the United States and are now being controlled by botnets*

Attack Profile

- Evolved from spam and denial-of-service attacks to attacks on websites for profit and to take down rival networks
- Profit from attacking a gambling website = US$50,000

Botnet Infection Process



Step 1:

Clients are infected by spyware, malware, and targeted attacks propagated by web and email

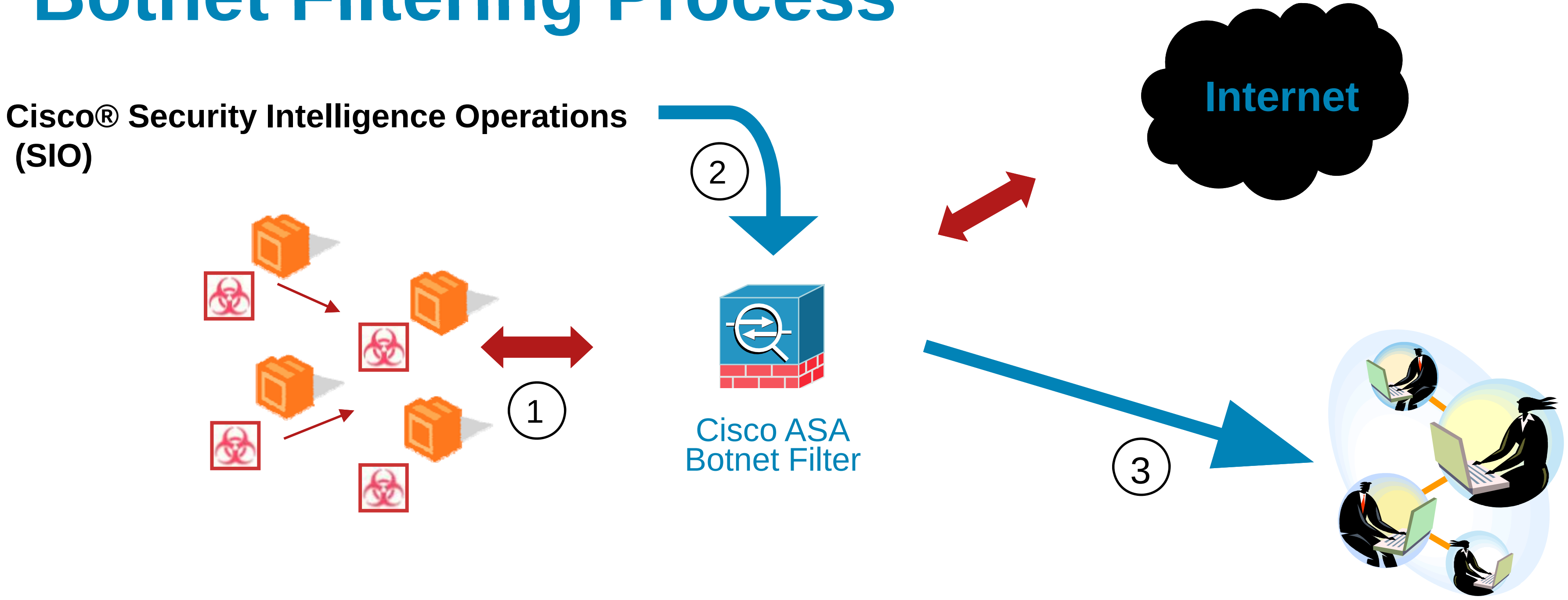
Step 2:

Infected clients communicate with a command and control host on the Internet

Step 3:

Attacks are launched: DoS, ID theft, spam, and click fraud

Botnet Filtering Process



Cisco® Security Intelligence Operations (SIO)

Step 1:

Infected clients try to communicate with a command and control host on the Internet

Step 2:

Cisco SIO updates the Cisco ASA botnet filter list; the destination is a known attack site

Step 3:

Alerts go out to the security teams for prevention, mitigation, and remediation

Botnet Traffic Filter

Client Infection Detection

- **Botnet traffic filter**

  Scans all traffic, all ports, and all protocols

  Monitors command and control traffic from internal bots to external hosts

  Detects infected clients by tracking rogue "phone-home" traffic

- **Powerful anti-malware data promotes accuracy**

  Provides guidance now for blocking Botnet communication

  Dynamic discovery provides real time identification of malware communication

Cisco Security Innovation

Anti-Malware

Cisco® ASA

Industry's Most Accurate Malware Traffic Monitor