



Security Technology Update



Ricky Elias
Security Architect
Advanced Technology (Security)
relias@cisco.com

Agenda

- Security Market Update
- SMB Market Opportunities
 - Endpoint Security with Data Leakage Prevention
 - Spam/Virus Blocker
- Q&A

Cisco Global Correlation

SensorBase: World's Largest Traffic Monitoring Network



Cisco Security Intelligence Operations

- Watchlist
- Manage Profiles
- Sources Monitoring
- Sources Report
- Filenames Grouping
- Profiles Grouping
- Rules
 - Rule Status
 - Create Rule
 - Create Rule (V2)
- Public Notes
 - Edit/Create—Notes
 - Edit/Create—Reasons
 - Map



Botnet Activity		
Botnet	Time	Nodes Detected
Srizbi	2009-07-23 09:47:27	302,672
Bobax	2009-07-23 09:16:33	183,939
Rustock	2009-07-23 09:35:38	153,532
Cutwall	2009-07-23 09:48:39	127,531

Calculating: ■■■■■

Email Traffic Alert		
IP Address	Vol.	Rep.
189.72.170.115	2.9	Poor
208.84.101.165	2.6	Poor
193.252.22.29	0.3	Good
212.214.213.238	0.3	Poor
76.162.254.116	6.9	Neutral
192.203.222.29	6.0	Neutral
82.116.25.7	0.1	Poor
222.124.18.72	2.1	Good

Threat Correlation	
Email	Web

Threat URLs		
Web Server	IP Address	Rep.
imp-porntube.net	64.27.28.224	Poor
www.Adware-Download.com	70.86.182.194	Poor
www.brothersoft.com	68.26.180.23	Poor
www.rocketdownload.com	38.102.33.137	Neutral
chennaiplus.net	208.113.167.238	Neutral
aeroflighttraining.com	66.96.130.122	Neutral

Threat Rule Publication			
Rule	Time	Platform	
URL (vlew/.exe)	2009-07-23 10:01:59	<input type="checkbox"/> All <input checked="" type="checkbox"/> Email	<input type="checkbox"/> Web <input type="checkbox"/> IPS
URL (insidevideo/.exe\$)	2009-07-23 10:02:02	<input type="checkbox"/> All <input type="checkbox"/> Email <input type="checkbox"/> Web	<input checked="" type="checkbox"/> IPS
CON (ch/gallery/\$\$\$/exe)	2009-07-23 10:02:09	<input type="checkbox"/> All <input type="checkbox"/> Email <input checked="" type="checkbox"/> Web	<input type="checkbox"/> IPS
URL (insidevideo/.exe\$)	2009-07-23 10:02:17	<input type="checkbox"/> All <input type="checkbox"/> Email <input checked="" type="checkbox"/> Web	<input type="checkbox"/> IPS
URL (video/php\$)	2009-07-23 10:02:23	<input type="checkbox"/> All <input type="checkbox"/> Email <input checked="" type="checkbox"/> Web	<input type="checkbox"/> IPS
MES (out/phon\$\$/bin)	2009-07-23 10:02:26	<input type="checkbox"/> All <input checked="" type="checkbox"/> Email <input type="checkbox"/> Web	<input type="checkbox"/> IPS

700,000+ sensors deployed globally

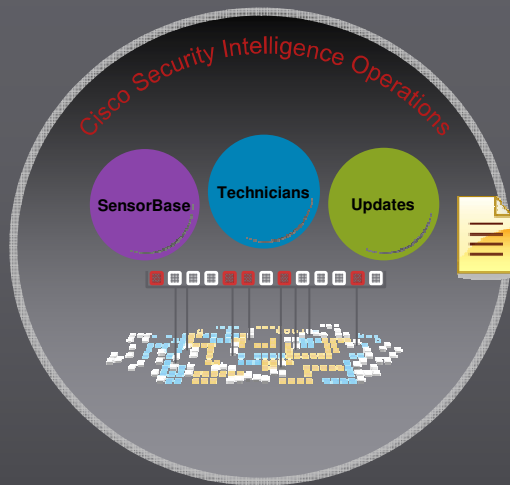
8 of the top 10 global ISPs

Over 500GB of data per day

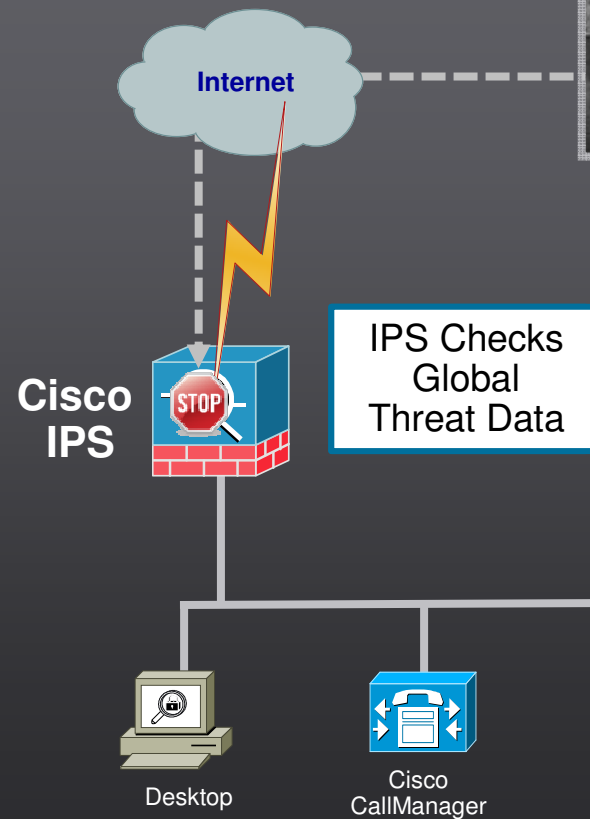
500 third party feeds

Over 30% of the world's email traffic

Cisco IPS with Global Correlation



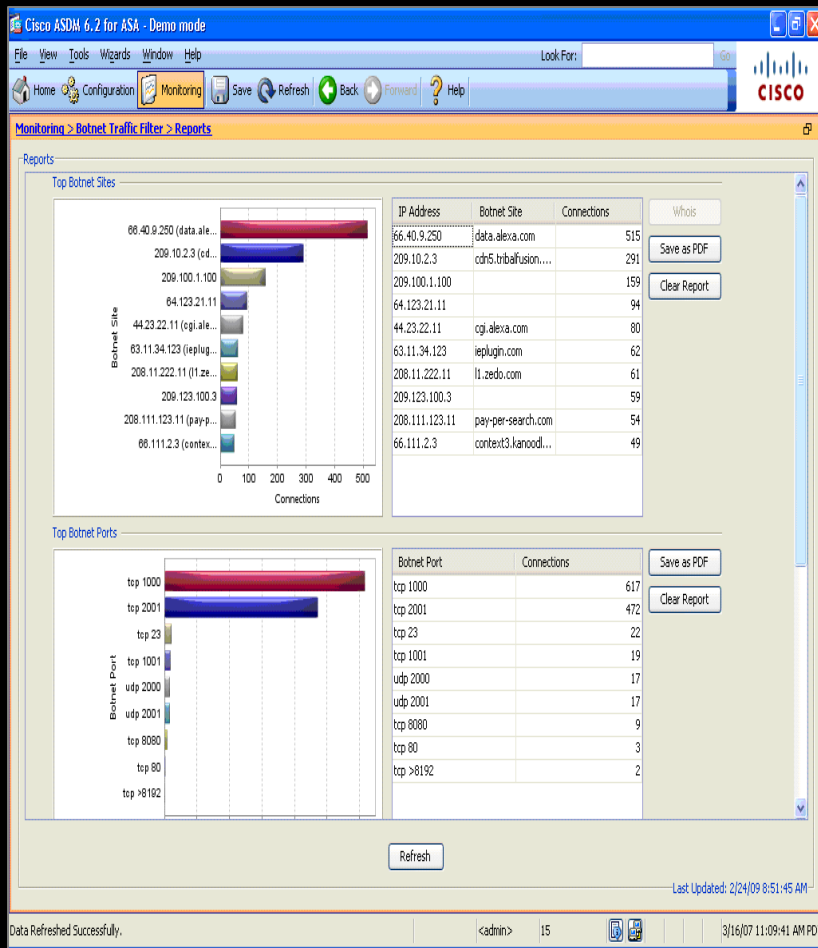
Attacker



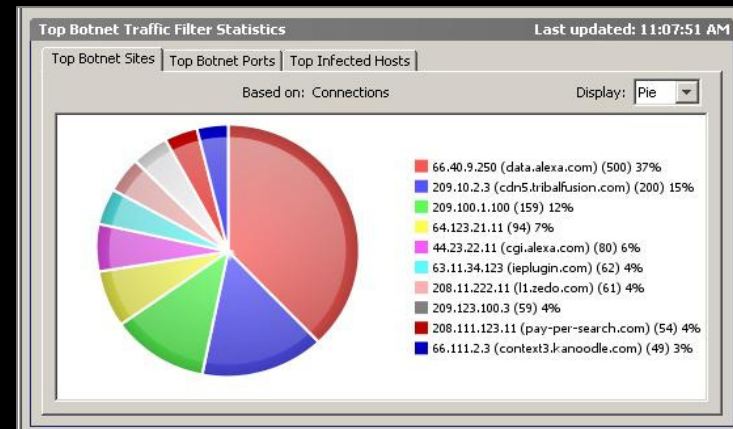
- **“Reputation” alone stops 10–15% of total attacks**
- **Benefits**
 - Stop attacks earlier
 - Automation increases security team productivity and effectiveness

Cisco ASA Botnet Traffic Filter

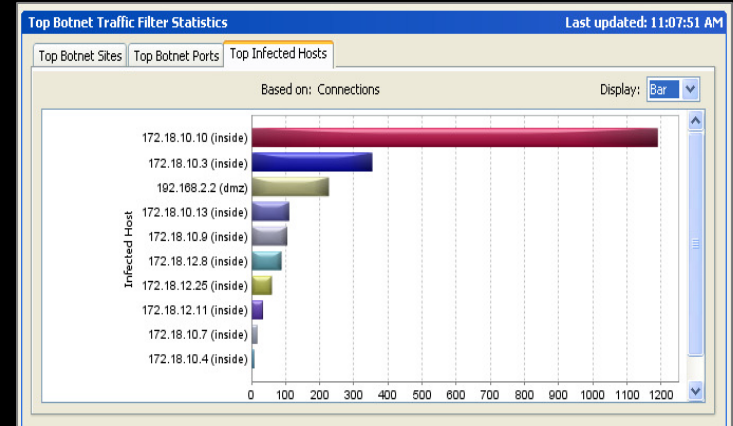
Top Botnet Sites, Ports and Infected Endpoints



Monitoring



Live Dashboard



Integrated Reporting

Endpoint Protection with DLP

Protecting Data In-Use

A Shift in Security Strategy for SMB

Forrester Research

Forrester: SMB security spending to increase in 2009

By Linda Tucci | Jan 9, 2009

IT executives at small and medium-sized businesses (SMBs) will spend a full percentage point more of their IT budgets on security in 2009 than 2008, according to a new study from Forrester Research. The change will result from **a shift in security strategy from computer security threat defense to corporate data protection.**

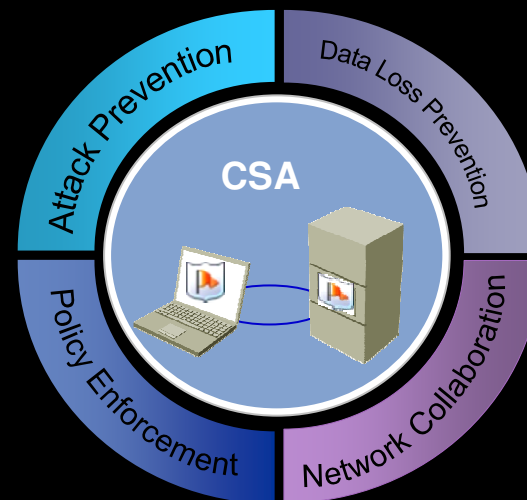
Nearly 20% of the respondents plan to pilot or adopt a host intrusion prevention system (HIPS), file-level encryption, full disk/desktop encryption, endpoint control and data leak prevention in the next 12 months. The moves will almost double the use of these security technologies at SMBs.

<http://www.searchsecurityasia.com/content/forrester-smb-security-spending-increase-2009>

Cisco Security Agent

Comprehensive, “Always Vigilant” Endpoint Security

- Single Integrated Client, Simplified Management
 - Host IPS, Personal FW, Anti Virus, Anti Spyware, Anti Botnet
- Protection against persistent and evolving threats
 - Prevent loss of sensitive information
 - Enforce appropriate use policies
 - Enhance security through network collaboration
 - Address corporate and regulatory compliance mandates



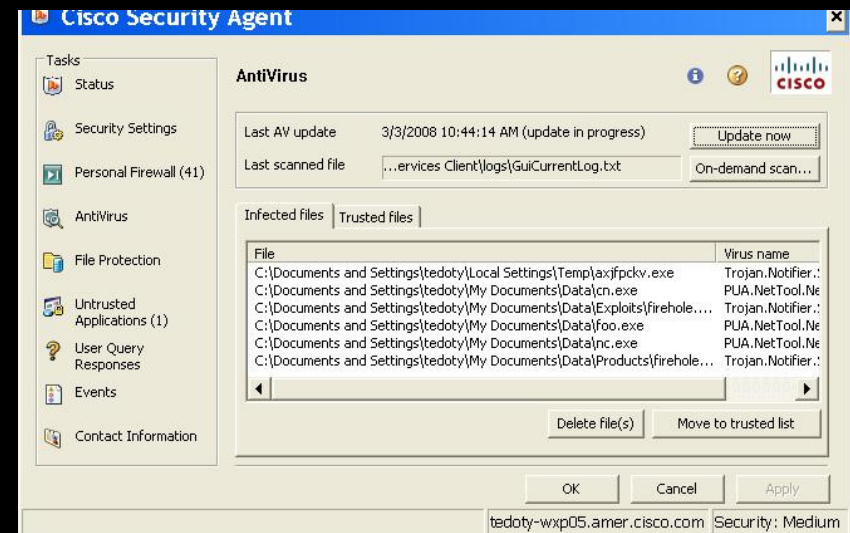
Business Benefits:

- Empower IT to address Business risks
- Enforce policies and protect business critical assets
- Decrease IT administrative burden
- Reduce expenses

Integrated Agent

with ClamAV™ Open Source Antivirus

- ClamAV virus scanning engine packaged with CSA, as single installable agent
- Protects Windows desktops & servers at no additional cost
 - accurately identifies malware
 - prevents malware execution
 - quarantines or deletes malware
- CSA Management Center manages agent policies, signature updates
- Provides a true single agent - single console endpoint security solution



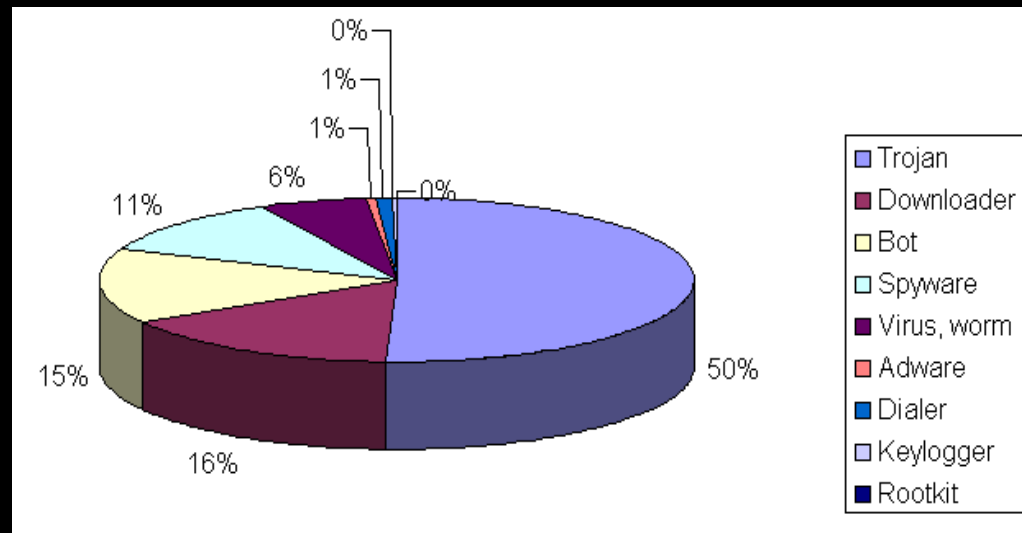
Integrated Agent with Clam Antivirus

- ClamAV is widely deployed on UNIX/Linux e-mail servers

Scrubs e-mail traffic for malware

Protects millions of Windows desktops

Database contains over 200,000 unique signatures



Shadowserver Foundation independent research: ClamAV™ has high degree of malware detection accuracy.

vendor	detected	total	percent
AntiVir	1204953	1229800	97.98%
Vexira	1203678	1229800	97.88%
VirusBuster	1203471	1229800	97.86%
F-Secure	1203244	1229800	97.84%
Norman	1203274	1229800	97.84%
F-Prot6	1202403	1229800	97.77%
Clam	1201805	1229800	97.72%
DrWeb	1201442	1229800	97.69%
AVG7	1200639	1229800	97.63%
Avast	1199011	1229800	97.50%
McAfee	1185278	1229800	96.38%
F-Prot	1176390	1229800	95.66%
Panda	1138986	1229800	92.62%
Kaspersky	1036869	1229800	84.31%
BitDefender	1036210	1229800	84.26%
VBA32	994177	1229800	80.84%
NOD32	798148	1229800	64.90%

Source: Shadowserver.org wild testing

Data Loss Prevention Management Process

Visibility and Control for Sensitive Information

Discover

- Classification
 - Credit card, Social Security #s
 - Intellectual property definitions

Monitor

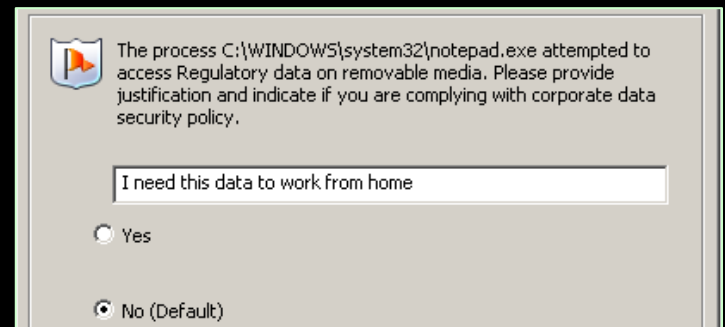
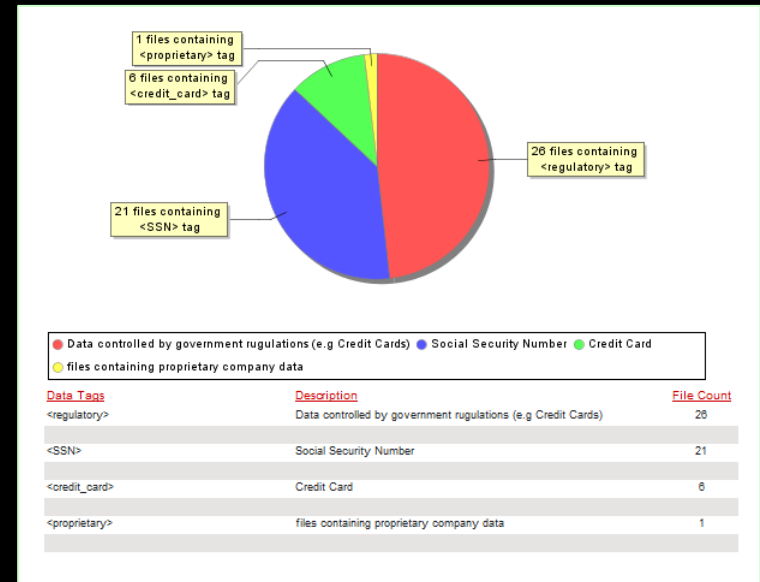
- Reporting
 - Track the location and usage of sensitive data

Educate

- Enhanced user education
 - Query user and audit

Enforce

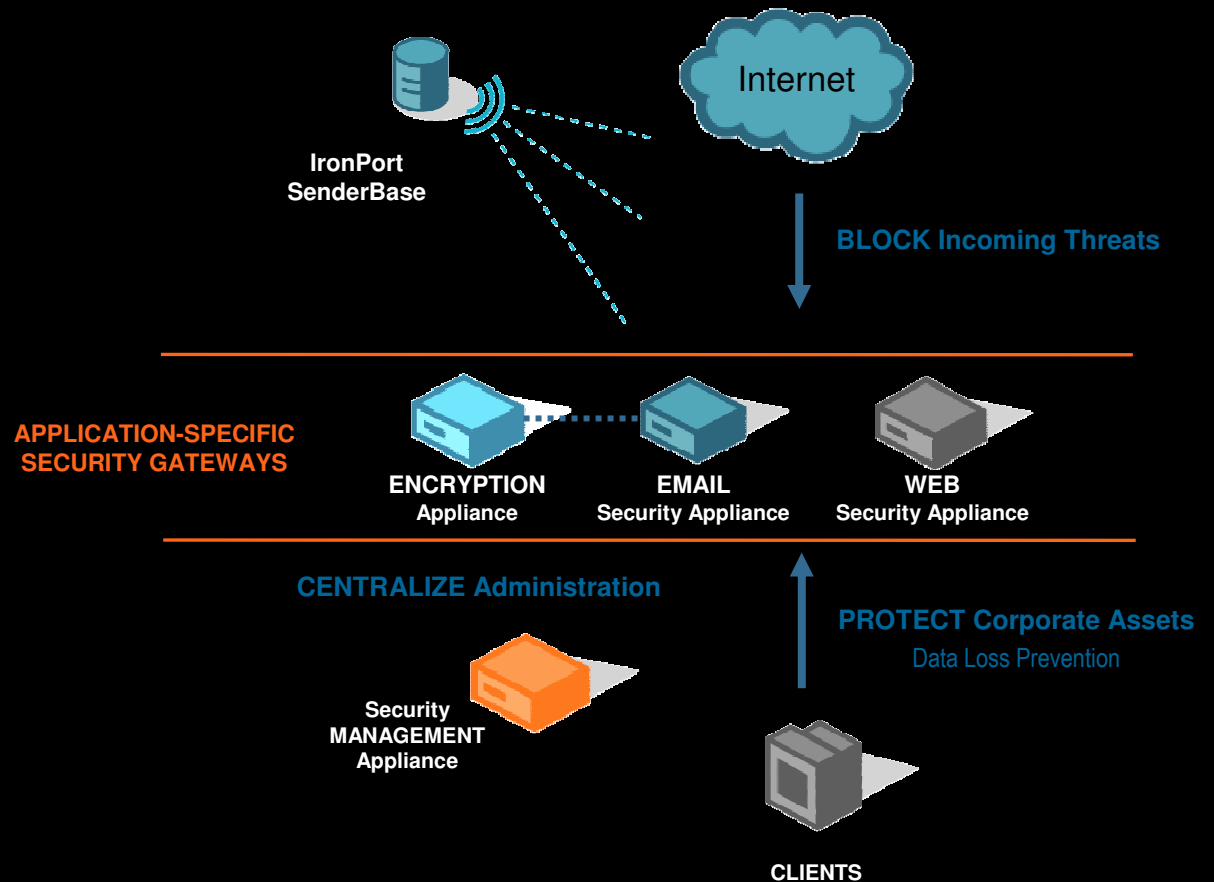
- Updated enforcement controls
 - Block printing
 - Flexible clipboard control
 - NAC quarantine



Spam/Virus Blocker

IronPort SensorBase Technology

IronPort Gateway Security Solution



Web Security Email Security Security Management Encryption

Cisco Spam and Virus Blocker

Immediate Protection Out of the Box

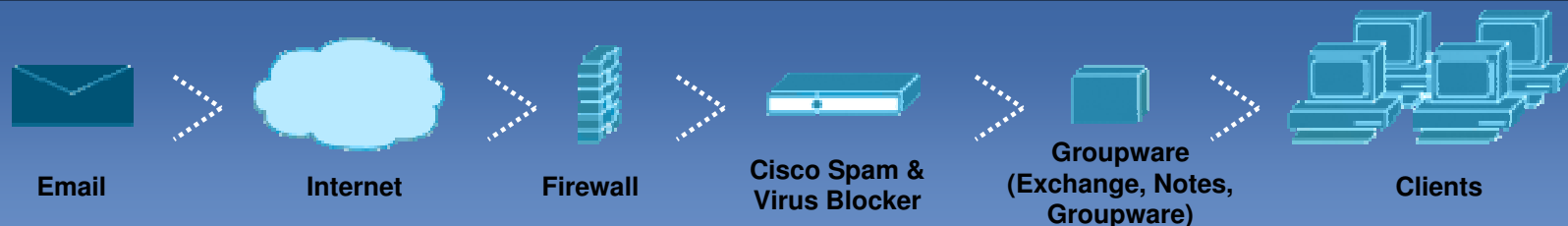


The Cisco Spam & Virus Blocker is a dedicated email security appliance for small business with up to 250 email users.

It provides powerful protection against spam, viruses and other email threats to secure your network and business data while improving productivity.

Reduces operational costs with simple setup in minutes and continuous automatic updates there after.

“Set it. Forget it. It just works.”



Customer Testimonial

Mirifex Systems



m i r i f e x
brilliant returns

“The setup wizard is fantastic! I could have given it to the receptionist and she could have set it up.”

IT Administrator
Mirifex

The screenshot shows the 'Cisco Spam & Virus Blocker' setup wizard. At the top, there are four steps: 1 License, 2 Registration, 3 Network (highlighted with a red box), and 4 Security. Below the steps is an image of the hardware device with labels for 'Data 1 (Default IP 192.168.42.42)' and 'Data 2 (Incoming Mail)'. The main content area is divided into three sections: 'Network Settings', 'Mail Configuration', and 'Administrator Settings'. The 'Network Settings' section includes fields for Blocker Hostname, Blocker IP Address, Subnet Mask, Gateway IP Address (set to 172.17.0.1), Time Zone (set to GMT), and DNS options. The 'Mail Configuration' section includes fields for 'Accept mail for these domains' and 'Exchange/Mail Server'. The 'Administrator Settings' section includes fields for 'Administrator Email' (ksnow@ironport.com), 'Your new administrator password', and 'Confirm your new password'. At the bottom, there are 'Previous', 'Cancel', and 'Next' buttons. The Cisco logo and copyright information are at the bottom of the page.

Four easy steps
Up and running
in less than 30
minutes

Benefit Highlight

Simplified Single SKU Ordering

- Bundles include everything (hardware, software, support) to simplify ordering to just one SKU.
- Available only through distribution and competitively priced.

Product Name		List (USD)
Point of Sale		
BLKR-SVB-50U-1Y	Cisco Spam & Virus Blocker - 50 User - 1 year	\$ 2,599
BLKR-SVB-100U-1Y	Cisco Spam & Virus Blocker - 100 User - 1 year	\$ 2,999
BLKR-SVB-250U-1Y	Cisco Spam & Virus Blocker - 250 User - 1 year	\$ 4,399
BLKR-SVB-50U-3Y	Cisco Spam & Virus Blocker - 50 User - 3 year	\$ 3,599
BLKR-SVB-100U-3Y	Cisco Spam & Virus Blocker - 100 User - 3 year	\$ 3,999
BLKR-SVB-250U-3Y	Cisco Spam & Virus Blocker - 250 User - 3 year	\$ 5,399
Renewal		
CON-BLK-BLKR50U	SW and Supp Subscr NBD Blocker 50 User (annual)	\$ 499
CON-BLK-BLKR100U	SW and Supp Subscr NBD Blocker 100 User (annual)	\$ 599
CON-BLK-BLKR250U	SW and Supp Subscr NBD Blocker 250 User (annual)	\$ 899

Build Customer Satisfaction

Comprehensive Support



Cisco Software and Support Subscription

Results

Proactive Anti-spam and Anti-virus Updates



Up-to-the-minute, industry-leading network protection virtually eliminates email threats from spam, viruses and other threats

Software Upgrades (Bug fixes, minor and major releases)



Maximum performance with the latest features

Cisco Small Business Support Center



Fast phone access, 365 days a year

Cisco.com Access



Online tools and resources help you solve issues, educate staff

Next Business Day Hardware Replacement



Resilient, reliable business operations

More Information



- Cisco Small Business Web Site: www.cisco.com/smallbusiness
- Cisco Partner Central – Security: www.cisco.com/go/smbpartner/security
- Cisco Spam & Virus Blocker: www.cisco.com/go/blocker
- Cisco Security Agent Web Site: www.cisco.com/go/csa
- Cisco DLP Solution Web Site: www.cisco.com/go/dlp





CISCO