Cisco Security Intelligence Operations

Insight into the Power of Cisco Security

Table of Contents

"These hackers aren't kids on a digital joyride. It's clear that their motive is financial gain."

Johannes Ulrich
SANS Institute

Today's distributed networks and an evolving security landscape bring an abundance of risk. Newly adopted tools and services, often untried and vulnerable, can be sabotaged or exploited for financial gain. Even strong security technologies are often unable to keep up with today's nimble, specialized, and targeted attacks. The consequences from security breaches include damage to a company's image, theft of personally identifiable information, service downtime, cleanup and remediation costs, compliance penalties, and corporate liability. The following threat statistics highlight the level of risk:

- Spam accounts for more than 100 billion messages each day — approximately 85 percent of the email sent worldwide. Eighty percent of spam is from infected clients.
- The number of disclosed vulnerabilities grew by 6.77 percent from 2007 to 2008.
- Vulnerabilities in virtualization products tripled to 103 in 2008 from 35 in 2007.
- Approximately 50 percent of attacks are committed by serial offenders. Approximately 70 percent of botnets use dynamic IP addresses to evade blacklists.
- Over the course of 2008, there was a 90 percent growth rate in threats originating from legitimate domains; nearly twice the amount of 2007.
- Organizations that experienced a data breach in 2008 paid an average of $6.6 million to rebuild their brand image and retain customers.

Many organizations have limited resources to deploy and maintain more technology, and to clean up after system compromises. They need a solution that can provide protection against evolving threats while reducing overhead costs.

Introducing Cisco Security Intelligence Operations

Traditional security products have provided protection by way of filters. With threat techniques continuing to increase in sophistication, these filters have to look deeper into network and application-layer traffic, and perform more processing on every byte. Unfortunately, this technique is not stopping malware and hackers: IT managers report they are spending more time than ever cleaning up infected PCs and servers, preventing data loss, and securing their networks.

It is not difficult to understand why deeper inspection with signature matching and behavioral analysis by itself is unable to handle the latest threats. The latest generation of malware uses multiple protocols, applications, and vectors to propagate. No two attacks are exactly the same: Binary containers, method of infection, and other attributes change each time they replicate.

Using layered defenses, with scanning engines from multiple vendors, does provide some incremental improvement in catch rates, but this is not enough to halt today's most sophisticated threats.

Cisco has responded with a system called Cisco Security Intelligence Operations (SIO).

Cisco SIO provides threat identification, analysis, and mitigation to continuously provide the highest level of security for Cisco customers. Using a combination of threat telemetry, a team of global research engineers, and sophisticated security modeling, Cisco SIO enables fast and accurate protection.

Cisco SIO delivers several completely new security technologies and enhances the filters already available in Cisco devices. Cisco SIO:

- Connects Cisco devices to a global view of emerging threats, so they can react faster to a wider range of security issues.
- Moves threat analysis beyond the packet and session levels, representing a seismic shift in how we can identify and respond to new security threats as they emerge, anywhere in the world.
- Gives customers the information they need to stay informed about the latest global threats and trends.

Cisco Security Intelligence Operations Overview

Cisco Security Intelligence Operations is a sophisticated security ecosystem consisting of three components:

1. **Cisco SensorBase:** The world's largest threat monitoring network captures global threat telemetry data from an exhaustive footprint of Cisco devices and services.
2. **Cisco Threat Operations Center:** A global team of security analysts and automated systems extract actionable intelligence from SensorBase data.
3. **Dynamic updates:** Real-time updates are automatically delivered to security devices, along with best practice recommendations and other content dedicated to helping customers track threats, analyze intelligence, and ultimately improve their organization's overall security posture.

Comprehensive Threat Intelligence

Cisco IronPort Systems began developing the SenderBase system in 2002. SenderBase was the world's first and largest email reputation tracking database. Now called SensorBase, the live database has become the world's largest real-time threat monitoring network, with:

- More than 700,000 (and growing) globally deployed Cisco security devices
- More than 40,000 vulnerabilities and 3300 IPS signatures
- More than 600 third-party threat intelligence sources, which track more than 500 third-party data feeds and 100 security news feeds around the clock

SensorBase collects a wide set of data to support more types of security filtering products, including data feeds from:

- Web security appliances (with new data about websites and URLs)
- Intrusion prevention systems (with new data about attacking hosts)
- Firewalls (with new data about botnets)
- Multivendor private and public sources

More than 1000 threat collection servers process 500 GB of data each day. The Cisco Threat Operations Center processes this global, real-time threat intelligence and incorporates it into the security services available on Cisco security devices, providing unrivaled protection.

SensorBase tracks data on more than 200 parameters, including the following sources:

- Public DNS registries
- Public IP ranges in use
- Public IP-to-geographic-region data
- Public blacklist and whitelist status on popular lists
- Public complaint data from SpamCop (a Cisco company)
- Contributed data from organizations such as Hotmail
- NetFlow - contributed volume data from large ISPs
- Sample emails from spamtrap (honeypot) accounts
- Email statistics from Cisco IronPort Email Security Appliance customers: volume, attachment types, antivirus and spam-check verdicts, and valid and invalid recipient counts
- Web traffic statistics from Cisco IronPort Web Security Appliance customers
- Public lists of compromised websites
- Public and private web volume data
- Website complaints reports
- Crawler data (Cisco spider or trawler programs that seek malware sites)
- Lists of URLs found in spam
- Alerts from IPSs and firewalls

The Cisco SIO system uses SensorBase data to boost the intelligence of Cisco devices.

Threat Operations Center

Cisco's powerful, automated algorithms process SensorBase data in real time. These tools generate about 95 percent of the rule updates used in Cisco devices. The remaining rules are hand-crafted and refined by threat analysts in the Threat Operations Center.

The Threat Operations Center teams consist of more than 500 people dedicated to 24x7x365 threat research, analysis, and quality assurance spanning five global locations.

A team of engineers is dedicated to packaging the rules into updates for various device types, testing those rules, and maintaining the advanced update delivery systems. A team of "white hat" engineers are experts in reverse engineering malware and other Internet threats. They infiltrate botnets as they are discovered by SensorBase, perform penetration testing, and research how malware works.

In addition to conducting research, threat operations teams also collaborate across Cisco and with Cisco customers to gather feedback and build secure products. These teams include:

Cisco SIO uses sophisticated algorithms to turn SensorBase data into actionable intelligence that is used by the Global Correlation engine.

- **Cisco IronPort Email and Web Threat Research Teams:** Provide the latest protection for SMTP and web-based attacks.
- **Cisco Malware Research Lab:** Focuses on researching the latest malicious activity.
- **Intrusion Protection Signature Team:** Researches and develops vulnerability and exploit-specific signatures that are used by IPS product lines.
- **Cisco Product Security Incident Response Team (PSIRT):** Evaluates and works across Cisco to mitigate vulnerabilities reported in Cisco products.
- **Strategic Assessment Technology Team (STAT):** Advanced, area-specific security research and product vulnerability testing.
- **Infrastructure Security Research and Development (ISRD):** Maintains security expertise and creates security solutions for customers engaged in emerging industries and infrastructures.
- **Remote Management Services (RMS):** Provides 24x7x365 remote monitoring and management of Cisco security devices that are deployed at customer sites.

- **IntelliShield Security Analysts:** Collect, research, and provide information about security events that have the potential for widespread impact on customer networks, applications, and devices.
- **Applied Intelligence Team:** Researches, documents, and tests potential mitigations for security-related advisories and bulletins from Cisco, Microsoft, and other vendors.

The Threat Operations Center provides the data that is used for outreach to the security community (www.cisco.com/security) and as the backbone for the Cisco IntelliShield Alert Service.

Global Threat Correlation

Cisco Global Threat Correlation is a sophisticated, automated security capability that enables Cisco security devices to respond to and protect against threats more quickly. Global threat correlation is checked against SensorBase threat information such as reputation, known exploits, anomalous behaviors, and vulnerability information to detect blended, widespread, and targeted attacks. Global Threat Correlation benefits from the complete visibility across all threat vectors gathered from SensorBase.

Whereas traditional network security systems examine only the packet contents, Global Threat Correlation performs a full-context analysis to better understand traffic — not just what the contents are, but who sent it, what it contains, where it came from, and how it has evolved. The following parameters are considered in the Global Threat Correlation engine:

- **Who:** The reputation of counter-party. Cisco IronPort Reputation Filters block the worst offenders, stopping 10 to 15 percent of attacks, and assigns an appropriate reputation to suspected attacks.
- **What:** The packet contents that match an exploit, virus, or vulnerability signature.
- **Where:** Geographic and vertical trends of the packets.
- **How:** The propagation and mutation methods.

Global threat correlation uses these parameters to continuously develop, test, and publish new rules to halt attacks more effectively, accurately, and quickly.

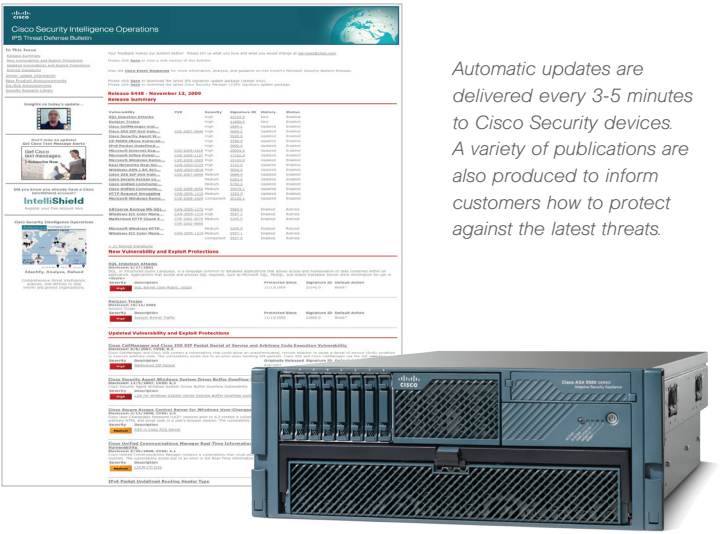
Dynamic Updates

Cisco SIO's dynamic updates deliver current and complete security information to Cisco customers and devices. Threat mitigation data is provided through:

- Automatic rule updates for Cisco products, such as firewall, web, IPS, or email devices
- IntelliShield vulnerability aggregation and alert services
- Security best practice recommendations and community outreach services

Some security updates are available in real time, such as reputation data that is used by Cisco security devices to block traffic from known malicious senders. Other systems, such as Cisco IPS with Global Correlation, query for new rules every five minutes.

Raw data is collected by SensorBase. The Threat Operations Center weights and processes the data. At this point, some of the data is ready to be used directly by Cisco devices. Other services and filters will push or pull specific Cisco SIO rule sets according to their settings. This interaction between devices and Cisco SIO enables the advanced protection and enforcement.



Automatic updates are delivered every 3-5 minutes to Cisco Security devices. A variety of publications are also produced to inform customers how to protect against the latest threats.

These interactions can occur in real time. Here's an example:

- A Cisco IronPort Email Security Appliance receives an incoming connection request.
- Instead of completing the TCP connection, it holds the connection half-open.
- The appliance sends a reputation request to SensorBase. (This is a DNS query on the remote IP address.)
- SensorBase returns a text record with a reputation score.
- Based on policy settings, the appliance might:
    - Drop the half-open connection (TCP Refuse).
    - Complete the connection and inform the sender their mail won't be accepted (SMTP Conversational Reject).
    - Whitelist the mail, skipping any spam checks for high-reputation senders.
    - Accept the mail normally and scan for spam.

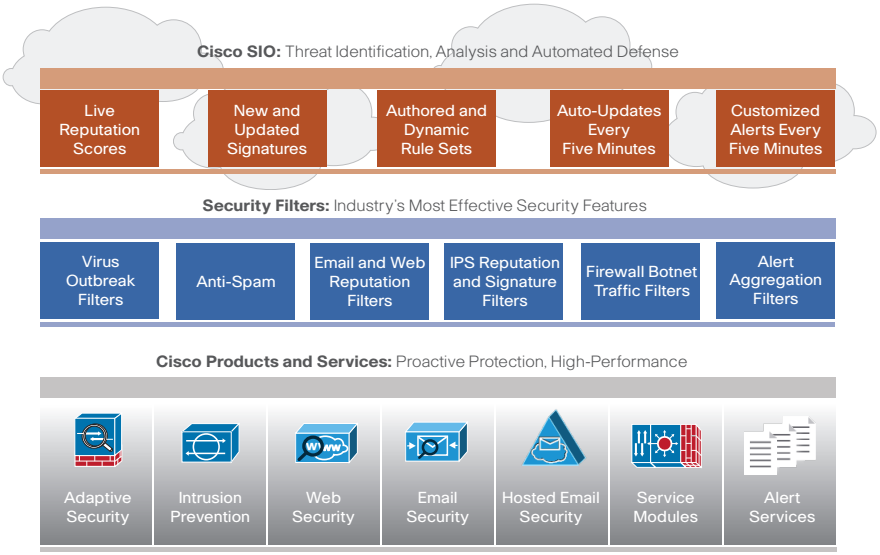
The reputation score is pulled directly from SensorBase. The Threat Operations Center is responsible for weighting the 200+ parameters in SensorBase that relate to the trustworthiness (credit rating) of this email sender. The Cisco IronPort Email Security Appliance was protected without having to scan the message. The decision to drop can be made before the messages are received, saving bandwidth and processing time.

Advanced Cisco SIO protection is available on the following Cisco products:

- Cisco Adaptive Security Appliances
- Cisco IronPort Email Security Appliances, Hosted Email Security, and Hybrid Hosted Email Security
- Cisco IronPort Web Security Appliances
- Cisco Intrusion Prevention Systems
- Cisco Integrated Services Modules
- Cisco IntelliShield Alert Services

These devices and hosted services are licensed with one or more security filters that are powered by Cisco SIO, including:

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



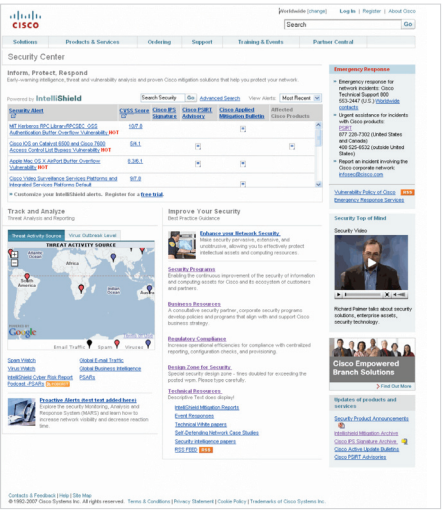
Cisco SIO provides the information and updates used by Cisco Security devices. The devices are equipped with innovative security filters, providing accurate and effective coverage.

Publications

In addition to dynamic updates, Cisco's security intelligence is represented in many forms for the benefit for the general public, end customers, enterprises, and even governments. Further examples of Cisco's security intelligence include:

- Cisco IntelliShield Alerts, including Malicious Code Alerts, Security Activity Bulletins, Security Issue Alerts, and Geopolitical Security Reports
- Cisco PSIRT Security Advisories and Security Responses
- Applied Mitigation Bulletins
- Cyber Risk Reports
- Security Intelligence Best Practices
- Service Provider Security Best Practices
- Cisco IPS Threat Defense Bulletins
- Cisco Event Responses
- Cisco Annual and Midyear Security Reports
- Cisco Threat Outbreak Alerts

Through this comprehensive approach to understanding and combating threats, you gain the knowledge you need to make educated decisions about increasing your security posture and ensuring that your network is automatically protected from the latest attacks.



The Cisco Security Intelligence Operations Portal provides the latest multi-vendor threat and vulnerability information and best practices to keep the security community up to date on the latest security risk.

"Ten years of compelling data clearly indicates the virus problem shows no sign of abating. Real progress will be made when companies rely less on defensive technologies and more on proactive security polices and practices."

Larry Bridwell
Content Security Programs Manager, ICSA Labs

How it Works

You can think of Cisco SIO as the command and control center — the brains of this ecosystem. But the intelligence is distributed, and devices interact with each other as well as with the central functions. Cisco SIO operates in three ways.

Device-to-Cisco SIO and Cisco SIO-to-Device

First, Cisco devices act as the enforcement points in this ecosystem — they use the Cisco SIO filters to block traffic. They also contribute threat intelligence and data back into Cisco SIO. So they get rules and reputation data at the same time they're making contributions to it. Just by making reputation queries, customers are contributing to the volume data. A small percentage of customers disable their network participation, but, for most customers, their use of Cisco SIO is bidirectional and improves their local catch rate and reaction time.

Device-to-Device

A second way that Cisco SIO works is within a corporate network. When one device in the network detects an event or a rule fires, that device may be able to inform other Cisco devices in that network. An IPS sending an ACL to a firewall is an example of this. Not all customers permit this level of Cisco SIO integration, but it does ensure faster responses to new threats.

Alerts and device-instigated rule changes are unidirectional. Cisco intends to offer additional modes, so that if one device detects suspicious activity, it may intelligently redirect traffic or alert other devices so that they can start scanning in much greater depth. Good traffic can be let through, bad traffic can be blocked, and suspicious traffic can be redirected for further processing. For example, if a Cisco ASA 5500 Series Adaptive Security Appliance detected unusual HTTP sessions, it could use Web Cache Control Protocol (WCCP) to redirect the sessions to a Cisco IronPort Web Security Appliance for malware scanning by Webroot and McAfee.

This will make it possible to perform application-layer, in-depth scanning even at multi-gigabit data rates, and should remove concerns about the performance impact of security scanning.

"Cisco IronPort Virus Outbreak Filters is a big winner for us. We know that our network is protected, even as we wait for traditional anti-virus signature updates."

Mark Dial
E-Messaging Team Manager, Tellabs, Inc.

Global Correlation Mode

Cisco SIO works in a third, more global way. When new threats are detected in one customer network, that data is shared with Cisco SIO, and then, indirectly, with other Cisco customers around the globe. Cisco SIO is already the world's largest global security ecosystem. The near-real-time, bidirectional cooperation of these networks means that Cisco customers protect each other.

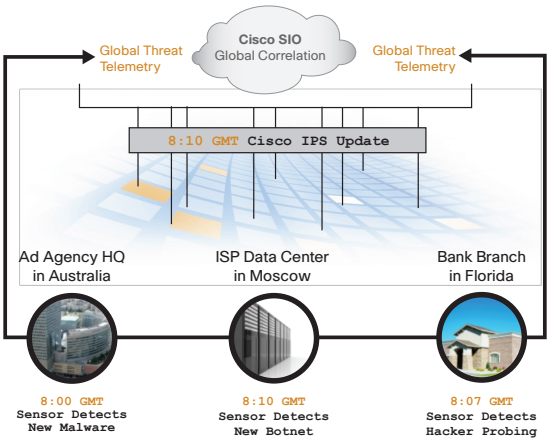
Examples of Cisco SIO in Action

The best way to understand how Cisco devices interact with Cisco SIO and receive advanced protection is to walk through a few examples.

Example: Global Correlation in IPS

The following example outlines how Cisco IPS with Global Correlation protects against new, emerging threats hours — and sometimes days — before traditional IPS signatures are released.

1. IPS sensors are located in four customer networks: in Australia, Russia, and Florida.
    - They are all receiving regular updates from Cisco SIO, in the form of signature-based rule sets for Cisco IPS sensors.
    - They all provide network participation data and alerts to Cisco SIO.
2. At 8 a.m. in the middle of the week, the Australian customer's sensor detects a new type of malware that doesn't match any known signature. It passes this data to Cisco SIO.
3. At the same time, the Russian customer's sensor detects botnet command and control traffic going to a previously unknown site.
4. The sensor in Florida detects a hacker probing open ports at major financial institutions.
5. Although none of these events triggers an exact match in the current IPS signature database, Cisco SIO creates new dynamic rules for IPSs.



In this example, Cisco IPS with Global Correlation detects threats propagating in various countries and creates a new ruleset within 5 minutes to protect against the emerging threat.

6. By 8:15 a.m. all Cisco IPS customers, including the three above, have received a dynamic rule update, and are protected from these new threats.

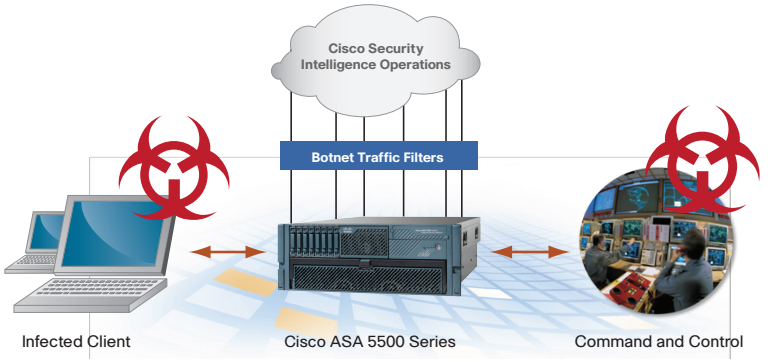
Without Cisco SIO, IPS customers may receive signature updates once or twice per week, and they are unprotected until the next update. With Cisco SIO, data about attacks seen by one network are passed into SensorBase, where the Threat Operations Center automatically generates new dynamic rules. Within a few minutes, Cisco SIO delivers these to Cisco customers around the globe, and their networks are able to block the new threats.

Example: Multi-Device, Multi-Protocol Protection

The following example outlines how Cisco SIO correlates data about a threat affecting one protocol, such as SMTP, and uses the information to protect other protocols, such as HTTP.

1. A customer network contains a Cisco Adaptive Security Appliance, Cisco IronPort Email Security Appliance, Cisco IronPort Web Security Appliance, and IPS Sensor. Current rule sets are available in all appliances.
2. On November 5, 2008, unsolicited emails were sent out, inviting readers to watch the Obama victory speech. Links in the messages pointed to a spoofed government site, america.gov. Cisco IronPort Email Security Appliances with Cisco IronPort Anti-Spam blocked these emails based on existing rules, and uploaded data about the new spam to Cisco SIO.
3. Many unprotected mail recipients read the mail, followed the links, and were prompted to install a fake Flash player update, which infected their PC with malware and transmitted their passwords to the Ukraine.
4. The Cisco customer network automatically received new rule sets blocking access to multiple computers hosting the spoofed site and malware.
5. When protected users tried to access the three botnet URLs, they were blocked.

Multi-device, multi-protocol protection is critical now that most attacks are blended threats, using multiple vectors and protocols, as well as fast-flux techniques involving a rapidly changing set of zombie PC hosts. Firewalls



Cisco's Botnet Traffic Filters find a compromised endpoint by detecting phone home traffic to a command and control host.

and other security devices must share an "awareness" of new threats and automatically provision new rule sets to mitigate these threats. A layered defense that only relies on multiple scanning engines may not be able to pick up these new threats until many systems are infected.

Example: Interdevice Protection

The following example outlines how Cisco SIO helps Cisco devices cooperate with researchers and protect Cisco Security networks around the world.

1. On Tuesday, December 9, 2008 (a Microsoft Patch Tuesday), anomalies in the alert and log data coming from Cisco IPS Sensors, as well as an unusual amount of NetFlow data, were escalated to the Cisco Threat Operations Center.
2. Analysts found the command and control hosts for a new botnet that was exploiting a known Internet Explorer vulnerability, affecting many sites with unpatched PCs. The Threat Operations Center was quickly able to modify the botnet rule set.
3. Automatic botnet traffic filters were published for customers with Cisco IronPort Web Security Appliances and Cisco Adaptive Security Appliances, and critical warning notices were made available to Cisco IntelliShield customers, independent software vendors, and the general public.

Cisco SIO Customer Validation

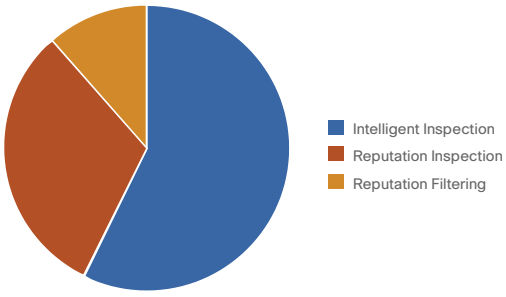
Here are just a few of the ways that Cisco SIO proves itself in real customer networks:

- Cisco IPS customers reported that with reputation and signature filters enabled, their appliances detected twice as many threats.
- Cisco IronPort Email Security Appliance customers reported that reputation filtering lets their appliances block 90 to 98 percent of spam at the connection level, before it is received. This is double the block rate of the closest competitor.
- Customers using Cisco IronPort Virus Outbreak Filters can quarantine email messages with attachments if Cisco SIO reveals a zero-day outbreak. The Threat Operations Center constantly tracks how quickly the six most popular antivirus vendors release signatures for new threats, and Cisco IronPort Virus Outbreak Filters reacts an average of 13 hours faster. This gives Cisco customers 13 hours of additional protection that isn't available using layers of signature-based defenses.
- Cisco Adaptive Security Appliance customers can report on infected PCs in their network that "phone home" to malware sites. The Cisco appliances receive current botnet rule sets from Cisco SIO. No other vendor currently offers this capability.

Average Response Times of Anti-Virus Vendors

Hrs:Mins	Anti-Virus
06:51	Kaspersky
08:21	Bitdefender
08:45	Virusbuster
09:08	F-Secure
09:16	F-Prot
09:16	RAV
09:24	AntiVir
10:31	Quickheal
10:52	InoculateIT-CA
11:30	Ikarus
12:00	AVG
12:17	Avast
12:22	Sophos
12:31	Dr. Web
13:06	Trend Micro
13:10	Norman
13:59	Comman
14:04	Panda
17:16	Esafe
24:12	A2
26:11	McAfee
27:10	Symantec
29:45	InoculateIT-VET

Percentage of Packets Blocked



What are the Benefits of Cisco Security Intelligence Operations?

Cisco SIO helps businesses:

- Avoid unnecessary cleanup costs
- Protect their brand reputation
- Increase uptime
- Speed growth by embracing new technologies
- Optimize operational efficiency
- Increase their compliance posture
- Gain visibility into the latest threat landscape
- Improve protection against new and emerging threats by increasing the effectiveness of security devices
- Increase spam and threat prevention through higher detection accuracy

Why Cisco?

With the increase in blended, cross-protocol, and cross-vendor vulnerability threats, the security industry has come to recognize that point defenses, which provide protection from individual threats or for individual products, are no longer enough. Integrated security management, real-time reputation assessment, and a layered, multipoint approach are needed.

As infrastructures become more distributed, increased risk is inevitable. Cisco SIO enhances the ability to identify, analyze, and mitigate today's threats. Cisco is committed to providing complete security solutions that are integrated, timely, and effective — enabling pervasive security for organizations worldwide.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

C02-570820-00