

## CISCO IPS SENSOR SOFTWARE VERSION 5.0

### PRODUCT OVERVIEW

Cisco<sup>®</sup> IPS Sensor Software Version 5.0 delivers inline intrusion prevention to protect your network from known and unknown attacks. Part of Cisco's intrusion prevention solution, Cisco IPS Sensor Software Version 5.0 provides the intelligence to accurately detect, classify, and stop malicious applications, viruses, worms, and spyware/adware, before they can affect your network. Using unique Multivector threat identification algorithms, Cisco IPS Sensor Software Version 5.0 identifies an extensive range of attacks using multiple inspection and classification capabilities. Cisco's accurate intrusion prevention system (IPS) technologies stop malicious traffic through the use of correlation and validation tools, protecting valuable business-critical data and resources without the fear of dropping valid traffic. Cisco IPS Sensor Software Version 5.0 is available on Cisco IPS 4200 Series appliances and on the Cisco Catalyst<sup>®</sup> 6500 Series Intrusion Detection System Services Module (IDSM-2).

### NEW FEATURES

New Features of Cisco IPS Sensor Software Version 5.0 include:

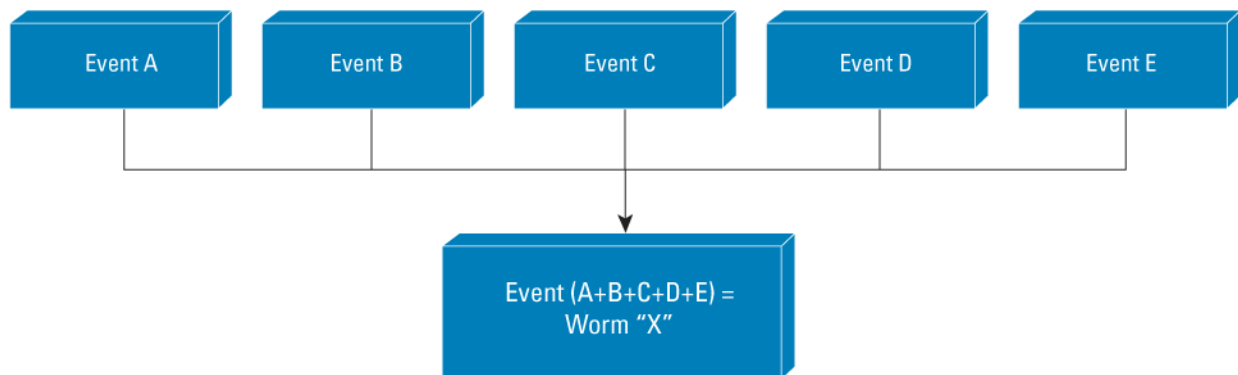
#### IPS Services to Stop Worms and Viruses

- IPS capability delivered to Cisco IPS 4200 Series appliances and the Cisco Catalyst 6500 Series IDSM-2, allowing effective worm and virus mitigation at strategic points across the network.
- Support for hybrid IDS/IPS services that allow a single sensor to operate simultaneously as an IDS sensor and an IPS sensor.
- Numerous packet drop actions to stop attacks.

#### Accurate Prevention Technologies

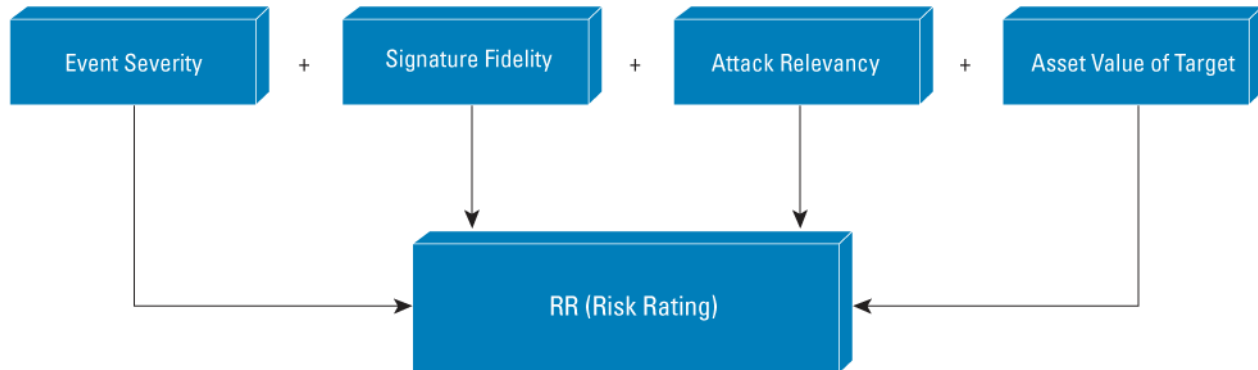
- Automated alarm aggregation for accurate worm classification and mitigation delivered through on-box correlation—the Cisco Meta Event Generator (MEG) (Figure 1).

Figure 1. Cisco Meta Event Generator



- Increase in the accuracy and confidence of IPS packet drop actions through a risk-balanced approach to classify threats. In contrast to traditional IPS solutions that depend on a simplistic model that only considers the IPS event severity rating, the Risk Rating allows the user to make more informed worm mitigation decisions through visibility into a variety of parameters that include: the severity of the event, relevancy of the attack, asset value of target systems, and fidelity of signatures (Figure 2). The result is a numerical risk rating that is automatically aggregated for the user and ensures that worm activity is stopped without dropping valid traffic.

**Figure 2.** Risk Rating to Enhance the Accuracy of IPS Actions



### Extensions to Multivector Threat Identification

- Protection from spyware and adware by allowing organizations to safeguard the integrity of sensitive information that can be divulged by malicious spyware applications as well as common adware such as Gator, Bonzi Buddy and SaveNow. Cisco IPS v5 contains unique algorithms that can effectively stop communications between spyware host servers and network devices that have been infected by spyware. Additionally, Cisco IPS v5 can also block unwanted communications generated by common adware applications.
- Application inspection technologies allow enforcement of policy decisions based on content detected at the application layer.
- Detection and prevention of covert channel tunneling through Port 80.
- RFC compliance checking for HTTP methods.
- Filtering of traffic based on malicious MIME types such as JPEG extensions.
- Control of permitted traffic via user-defined policies, such as the denial of Peer to Peer traffic that can potentially consume precious network bandwidth.
- Voice over IP (VoIP) engine to help ensure protocol compliance of H225 call setup messages. This engine also delivers protection against attacks to voice gateways through advanced buffer overflow and URL overflow mitigation.
- Support for the inspection and mitigation of threats in Multiprotocol Label Switching (MPLS) environments.
- Network antivirus capabilities to accurately identify and prevent virus outbreaks.
- Support for advanced traffic normalization algorithms such as fragmentation reassembly.
- Ability to identify attacks in IPv6 environments through the inspection of IPv4 traffic being tunneled in IPv6.

### Other Features

- Support for Security Device Event Exchange (SDEE), a standardized IPS communications protocol developed by Cisco for the IDS Consortium at ICSA.
- Extension of monitoring and notification mechanisms through the delivery of sensor alerts via Simple Network Management Protocol (SNMP) traps.

### UPGRADE PATHS

- Cisco IPS Sensor Software Version 5.0 will be shipped with all new Cisco IPS platforms.

- Cisco IDS or IPS sensors\* under a valid Cisco SMARTnet® contract may be upgraded to Cisco IPS Sensor Software Version 5.0 at no extra charge.
- Cisco IDS or IPS sensors\* that are not under a Cisco SMARTnet contract may be upgraded through the purchase of the following part number: IPS-SW-K9-U

## AVAILABILITY

Cisco IPS Sensor Software Version 5.0 will be available in March 2005.

## ORDERING INFORMATION

**Table 1.** Ordering Information for Cisco IPS Sensor Software Version 5.0

Part Number	Description
IPS-SW-K9-U	Cisco IPS Sensor Software Version 5.0

## FOR MORE INFORMATION

For more information about Cisco IPS Sensor Software Version 5.0, contact your local account representative or visit:

<http://www.cisco.com/go/ips>

\*Cisco IPS Sensor Software Version 5.0 is supported on the Cisco IDS 4215, IDS 4235, IPS 4240, IPS 4255, and IPS 4250-XL appliances and on the IDSM-2. It is supported in the promiscuous-based IDS mode only, for the IDS 4210 and the Cisco IDS Network Module (NM-CIDS).

Inline IPS services require more than one monitoring interface on Cisco IPS 4200 Series sensors.



### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

### European Headquarters

Cisco Systems International  
BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

### Asia Pacific Headquarters

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

