PRODUCT BULLETIN NO. 2706

CISCO THREAT DEFENSE BUNDLES

DELIVERING COMPREHENSIVE THREAT DEFENSE FOR SMALL AND MIDSIZE BUSINESSES

Individually investigating alarms and mitigating attacks and their potential damage is no longer an effective strategy for busy networks. With the prolific nature of worms, viruses, and application attacks, business continuity relies on proactive security solutions that stop malicious traffic, protecting valuable data and information infrastructures.

Today, the technology to mitigate these threats is mature and readily available to small and midsize businesses (SMBs) through the Cisco Systems® Threat Defense bundle of network and host intrusion prevention system (IPS) software.

NETWORK INTRUSION PREVENTION

The Cisco IPS solution provides one of the first lines of defense against network attacks. Cisco IPS Sensor Software Version 5.0 accurately identifies, classifies, and stops malicious traffic before it affects business continuity, protecting your data and information infrastructure. Cisco IPS Sensor Software provides accurate and proactive protection through its multi-vector threat identification, which analyzes network data flow and protects your network by accurately inspecting and identifying malicious applications, worms, and viruses in real time. Cisco surpasses traditional prevention systems with the integration of accurate prevention technologies, stopping attacks before they occur. These technologies allow system administrators to stop a broader range of threats without the risk of dropping legitimate traffic. In addition, Cisco's IPS solutions collaborate with the network providing enhanced scalability and resiliency, including efficient capture techniques, load balancing capabilities, and encrypted traffic inspection.

The Cisco Threat Defense bundle is built around the Cisco IDS 4215 Sensor, a one-rack-unit (1-RU) inline sensor that delivers 80 Mbps of full-featured intrusion protection that can be deployed to monitor multiple T1 and T3 environments (Figure 1).

Figure 1. The Cisco IDS 4215 Sensor

HOST INTRUSION PREVENTION

At the endpoint, the deployment of a host IPS provides protection against both worms and viruses. The host IPS monitors processes on the host using a database of system policies. Rather than focusing exclusively on the attacks that are seen in the reconnaissance phases of network attacks, a host IPS approaches the problem from the other direction, preventing malicious activity on the host by focusing on behavior. By changing the focus to behavior, damaging activity can be detected and blocked—regardless of the attack.

Cisco Security Agent uses predefined and configurable security policies to determine whether a particular action or behavior is permitted. These policies are stored on a central management console that is tightly integrated with the CiscoWorks VPN/Security Management Solution (VMS). The Cisco Security Agent Management Console provides a central location where policies can be defined and downloaded by Cisco Security Agent

when the manager is polled. Cisco Security Agent requires little or no environmental tuning, shipping with predefined policies that prevent most types of malicious activity from occurring.

For applications requiring access to system resources, the system calls are intercepted by Cisco Security Agent, which then compares them against a cached policy. The agent correlates this particular call with others made by that application or process, and correlates these events to detect malicious activity. If the request does not violate policy, it is passed to the kernel for execution. If the request does violate policy, it is blocked. An appropriate error message is passed back to the application, and an alert is generated and sent from the agent to the Cisco Security Agent Management Console.

CISCOWORKS VMS

Deploying intrusion detection and prevention requires the ability to manage IPS device configuration and Cisco Security Agent policies. It is critically important to be able to capture the alarms from these devices and to correlate the information that they relay in order to quickly identify and respond to potential security events. CiscoWorks VMS allows network administrators and personnel to configure IPS devices as well as Cisco Security Agent devices running on multiple hosts through a single, common interface. CiscoWorks VMS eases the configuration and management of these devices and agents throughout the network. In addition, the CiscoWorks VMS Security Monitor provides a singular interface that captures the alarms from these agents and devices and allows network personnel to investigate alarms in greater detail. By combining Cisco IPS Sensor Software, the Cisco Security Agent, and the CiscoWorks VMS software suite, Cisco provides SMBs with the tools necessary to see into their networks, identify attacks, and respond appropriately. Together, these tools allow SMB network personnel to proactively defend their networks against attack and to secure their businesses.

ORDERING INFORMATION

Table 1 lists ordering information for Cisco Threat Defense bundles.

Table 1. Ordering Cisco Threat Defense Bundles

Part Number	Description
IDS4215-CSA-BUN-K9	Cisco Threat Defense IDS 4215/Cisco Security Agent Bundle: • One Cisco IDS 4215 Sensor appliance • One Cisco Security Agent server • 10 Cisco Security Agent desktop agents • CiscoWorks VMS-Basic
CON-SNT-IDS4215B	Cisco SMARTnet® support for IDS4215-CSA-BUN-K9

EXPORT CONSIDERATIONS

Cisco Threat Defense bundles are subject to export controls. For export guidance, refer to the export compliance Website at:

http://www.cisco.com/wwl/export/crypto/

For specific export questions, contact: export@cisco.com

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.**

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

204107_ETMG_JT_11.04

Printed in the USA