

Cisco Intrusion Detection System

Delivering Proven Leadership and Technology Innovation

Cisco® Intrusion Detection System (IDS) is a component of the Cisco Threat Defense Security System, which minimizes the impact of both known and unknown threats through the collaboration of security and network intelligence services.

Cisco is a pioneer in the area of intrusion detection. As the first developer of network IDS technology, Cisco/WheelGroup shipped the first network IDS product in 1996. Since then, Cisco has continued to innovate and drive the market to mass adoption, through:

- **Patents**—Cisco has 10 patents awarded, with six additional patents pending formal approval (Table 1).
- **Automated response actions**—In 1996, Cisco/WheelGroup delivered the industry’s first automated shunning feature that enabled IDS sensors to reach out across the network and modify access control lists (ACLs) on routers to deny an attacker access to the network. In a subsequent release, this was enhanced to include switches and firewalls as devices that can also be managed by the sensor.
- **Router integration**—This was first executed to the strategy of ubiquitously integrating inline intrusion protection technology into the infrastructure in 1999. In 2003, this integration was enhanced through the delivery of a network module for Cisco access routers.
- **Switch line card**—Cisco delivered the first switch-integrated IDS module (IDSM-1) in 2000, securing the “Best-in-Show” honors at Network+Interop for extending the migration of this technology into the network fabric. In 2003, this innovation was enhanced by the delivery of a second-generation IDS module (IDSM-2), for the Cisco Catalyst® 6500 Series switch, designed to target higher bandwidths.
- **Firewall integration**—Cisco IDS technology was integrated into the market-leading Cisco PIX® Firewall in 2001, further extending pervasive coverage.
- **Attack identification and classification**—Cisco pioneered many of the advanced detection algorithms available today, using both signature-based and anomaly-based algorithms, including:
 - Stateful pattern matching, protocol parsing, heuristics, and anomaly detection.
 - Signature micro engines—Cisco released the industry’s first micro engine technology for attack identification and classification, allowing users to create and modify signatures using controlled development techniques. This technology also allows for rapid updates on signatures, as definitions are tied to dynamic signature modules, not application code.



- Custom signatures—Cisco IDS delivered Threat Analysis Micro Engine (T.A.M.E.) policy language. T.A.M.E gives users the flexibility to create new policies or modify existing policies to meet their unique security objectives.
- Active update technology—This allows users to rapid deploy and update sensors using secure and automated methods.
- **Threat validation**—Cisco Threat Response delivered patented technology in 2003 that works with IDS sensors to virtually eliminate false alarms, escalate real attacks, and aid in the remediation of costly intrusions through “just-in-time” analysis of target systems.
- **Inspection of encrypted network traffic**—Through collaboration with IP Security (IPSec) VPN and generic routing encapsulation (GRE) traffic, the network module introduced in 2003 for Cisco access routers allows decryption, tunnel termination, and traffic inspection at the first point of entry into the network—an industry first.
- **Multigigabit IDS load balancing**—In 2003, Cisco IDS delivered load-balancing capabilities for multigigabit IDS appliance deployments by using Cisco EtherChannel® load-balancing algorithms on the Cisco Catalyst 6500 Series. This allows Cisco IDS solutions to scale to meet high-aggregate throughput requirements, such as those found in large data centers.

Table 1 Awarded and Pending Patents for the Cisco IDS Product Line

| Patent # | Description |
|-----------|---|
| 6,405,318 | Intrusion Detection System |
| 6,609,205 | Network Intrusion Detection Signature Analysis Using Decision Graphs |
| 6,487,666 | Intrusion Detection Signature Analysis Using Regular Expression and Logical Operators |
| 6,578,147 | Parallel Intrusion Detection Sensors with Load Balancing for High-Speed Networks |
| 6,324,656 | System and Method for Rules-Driven Multi-Phase Network Vulnerability Assessment |
| 6,282,546 | System and Method for Real-Time Insertion of Data into a Multidimensional Database for Network Intrusion Detection and Vulnerability Assessment |
| 6,301,668 | Method and System for Adaptive Network Security Using Network Vulnerability Assessment |
| 6,499,107 | Method and System for Adaptive Network Security Using Intelligent Packet Analysis |
| 6,415,321 | Domain Mapping Method and System |
| 6,477,651 | Intrusion Detection System and Method Having Dynamically Loaded Signatures |
| Pending | Method and System for Maintaining Network Activity Data for Intrusion Detection |
| Pending | Method and System for Configurable Network Intrusion Detection |
| Pending | Method and System for Configurable Network Intrusion and Detection |
| Pending | Method and System for Adaptive Network Security Using Intelligent Packet Analysis |
| Pending | Method for Reducing the False Alarm Rate of Network Intrusion Detection Systems Using Active Fingerprinting techniques |
| Pending | Method for Reducing the False Alarm Rate of Network Intrusion Detection Systems Using Active Investigation Techniques |



Awards

- Computerworld: Reader's Choice Award 2003: Cisco IDS 4250
- Networking Industry Awards 2003, IDS Product of the Year: Cisco IDS 4250-XL
- Channel Champion's Award, 2003
- Information Security 2003 Excellence Award Finalist
- 2003 *Network Computing* Well-Connected Award Finalist: Cisco IDS 4250
- *Computerworld* Readers' Choice Awards Finalist, 2003
- *Network News* Editor's Choice Award, 2002
- CRN IDS Channel Champion, 2002
- *Network World* Blue Ribbon, 2001
- Networld+Interop Best of Show, 2000
- SC InfoSecurity 5-Star, 2000

Experience and Expertise—Thought Leadership

Network knowledge—Cisco is the undisputed leader in networking. Our experience and expertise allow us to deliver solutions that solve e-business problems.

Security knowledge—Cisco has been a thought leader in security for more than 10 years.

- **Products**—The Cisco Threat Defense Security System delivers the broadest portfolio of market-leading technologies spanning firewall; VPN; network-based IDS; host-based IDS; authentication, authorization, and accounting (AAA); and security management. The Cisco IDS team has more than 250 years of combined experience in network security.
- **Services**—Cisco has been offering security consulting services since 1995. Through this high-touch service, Cisco has acquired extensive knowledge of security, security postures, and vulnerability trends.

C-CRT—The Cisco Countermeasure Research Team (CRT) is a team of renowned security experts with more than 27 secret or top-secret government clearances and backgrounds in the USAF, National Security Agency, and the Central Intelligence Agency. This elite team of researchers develops and distributes countermeasure signatures to pre-empt electronic security threats found in the wild.

Market Leadership

- **#1 Security vendor**—Cisco is a dominant security vendor, with sales nearing \$1 billion. Cisco has market-leading products in each technology segment, including firewall, VPN, and IDS.
- **Security architecture**—Cisco was the first security vendor to develop a comprehensive security blueprint (the SAFE Blueprint) for building secure network environments. Cisco has best practices blueprints for enterprise, small and medium-sized businesses, VPN, voice, and wireless networks.
- **World-class support**—Cisco has award-winning product support solutions that provides worldwide, 24x7x365 support.
- **Rich partner ecosystem**—Cisco has a rich ecosystem of product and services vendors as part of the Cisco AVVID (Architecture for Voice, Video and Integrated Data) Partner Program. This program certifies the interoperability of partner products with Cisco technology, and verifies the services provided by these partners.

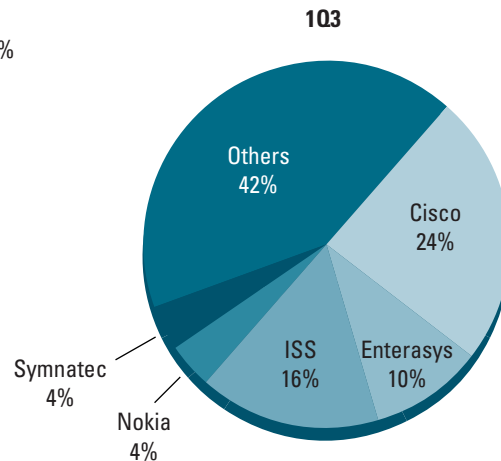


- **Market-share position**—Based on Infonetics Q1CY03 reports, Cisco IDS leads the industry with the #1 spot in the categories of Worldwide Network-Based Intrusion Detection and Prevention Product Market Share (Figure 1).

Figure 1

Cisco IDS: Marketshare Leadersip

Market Segment: \$73M
Cisco Market Share: 24%
Revenue Position: #1
Source: Infonetics



IDS in SAFE Blueprint

IDS is an element of the SAFE Blueprint from Cisco—a best practices security blueprint designed to launch e-business into the future. In practice, the SAFE Blueprint determines which security solutions you should deploy throughout your network via custom-designed modules that simplify security design, rollout, and subsequent management. The enterprise gets immediate and clear benefits from SAFE because the blueprint:

- Provides a solid foundation for migrating to secure and cost-effective converged networks
- Enables the cost-efficient deployment of a modular, scalable security framework in manageable stages
- Delivers truly integrated network protection with the highest-level security products and services

This pervasive security blueprint, in which the different components integrate with one another, provides a quicker, less-expensive deployment. This translates into faster time-to-market of your e-business applications and an optimal return on investment as revenues increase more rapidly from the applications.

Relevant Links for the SAFE Blueprint

SAFE: IDS Deployment, Tuning, and Logging in Depth

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a008009c8b6.shtml

A Security Blueprint for Enterprise Networks

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00801bc111.shtml

SAFE White Papers and Presentations

http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_package.html



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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
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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, EtherChannel, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R) ETMG 203149—BU 10/03