

## Cisco Security IntelliShield Alert Manager Service



In order to protect mission-critical business services from threats, organizations need timely, accurate, and credible security intelligence. However, with thousands of vulnerabilities reported each year, security personnel are constantly challenged to find the reliable, appropriate intelligence they need. The Cisco® Security IntelliShield Alert Manager Service provides the strategic, targeted security intelligence that customers need to proactively respond to potential threats and help ensure business continuity. With this service in place, IT security staff can spend less time searching for information and instead can focus on remediation and proactive protection.

### Challenge

The first step in organizations securing their IT infrastructure is understanding where threats and vulnerabilities exist. However, for each new security vulnerability discovered, organizations must know when the alert was released, how the network infrastructure could be impacted, and how the problem can be preemptively addressed. Finding reliable answers can take hours. That is because IT security personnel face:

- **Too much data**—Hundreds of public and private organizations report vulnerabilities each year. Security personnel often must search through dozens of mailing lists and Websites for data.
- **Too many formats**—New alerts can be published by dozens of different sources, each in its own format, using different processes to characterize, confirm, and report each problem.
- **Difficulty evaluating alerts**—With so many bodies publishing alerts, security staffs are challenged to find objective information about how critical a threat or vulnerability is to their environment.
- **Difficulty tracking remediation status and progress**—Few organizations have systems in place to effectively track the status of remediation efforts.



Multiply these problems by 5900—the number of vulnerability alerts issued in 2005, according to the independent security institute CERT\*—and the process of gaining reliable, appropriate security intelligence becomes a costly drain on IT security staff.

\*[http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html).

### **Solution**

Cisco Security IntelliShield Alert Manager is a threat and vulnerability alerting service that allows organizations to easily access timely, accurate information about potential threats and vulnerabilities in their environment—without time-consuming research. The service provides the comprehensive, cost-effective security intelligence organizations need to prevent, mitigate, and remediate potential IT attacks and more effectively help ensure business continuity and network availability.

Organizations using Cisco Security IntelliShield Alert Manager can customize the service by defining the unique networks, systems, and applications that make up their infrastructure, as well as criteria using a standardized risk rating system to determine the threats and vulnerabilities that affect them. The service then provides vendor-neutral intelligence alerts that are prefiltered to deliver only the relevant information, arming security personnel with the information they need to take rapid action and protect critical systems. As a result, security personnel can work more quickly and efficiently and can more effectively, prioritize remediation activities.

### **Business Benefits**

With the Cisco Security IntelliShield Alert Manager Service, organizations gain:

- **More efficient use of security staff resources**, because all alerts are delivered in a consistent, easy-to-understand format, and organizations receive only those alerts that affect their environment
- **More effective, timely security intelligence** via concise, easy-to-understand reports with proactive early warnings about new attacks and technology vulnerabilities
- **Higher-quality analysis**, because alerts are customized, preformatted, objective, vendor-neutral, and prioritized on a standardized risk-rating system
- **Faster remediation of potential vulnerabilities**, because many alerts include Cisco IntelliShield analysis of the threat with recommended safeguards and workarounds, as well as links to patches
- **Continuous protection against emerging threats and vulnerabilities**, because customers define the networks, systems, and applications that make up their infrastructure and customize the criteria and risk thresholds for receiving notifications, assuring that customers only see the information they need
- **Comprehensive threat and vulnerability information that covers the entire threat landscape**, including security vulnerabilities, malicious code, and global security trends that include historical information about thousands of vendors and products

### **Why Cisco**

Cisco Security IntelliShield Alert Manager is a pioneering security intelligence solution in the marketplace. The Cisco Security IntelliShield Alert Manager research team operates 24 hours a day, seven days a week to bring organizations current intelligence, as well as in-depth analysis and highly reliable threat validation. With Cisco Security IntelliShield Alert Manager, organizations gain more timely, effective, and comprehensive security intelligence—and greater ability to proactively defend their businesses—than ever before.

### **For More Information**

For more information about the Cisco Security IntelliShield Alert Manager Service, visit <http://www.cisco.com/go/intellishield> or contact your local account representative or your Cisco Systems® security partner.





**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.com Website 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



Copyright © 2006 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)