

---

## Cisco Products that Enable Federal Solutions

### **Cisco Security Agent: Protect Desktops and Servers and Enforce Security Policy**

Cisco® Security Agent software, for desktops and servers, provides threat protection by detecting anomalous application behavior and asking employees to confirm the action before permitting it. This provides another level of defense against spyware and bots, which federal agency managers identify as their top security concern. By looking for application behavior, not known virus signatures, Cisco Security Agent protects against unknown threats and new exploits and variants designed to take advantage of published and unpublished vulnerabilities. With this protection, agencies can patch on their own schedule, rather than constantly reacting to every new vulnerability. Cisco Security Agent can also improve risk management by prohibiting user actions that violate agency security policy, such as cutting and pasting or copying files to removable media. For more information, visit [www.cisco.com/go/securityagent](http://www.cisco.com/go/securityagent)

### **Cisco Security IntelliShield Alert Manager Service: Single Source for New Threat Information**

Agency IT groups often do not have the time to evaluate the credibility, urgency, and severity of new threat and vulnerability reports in different formats, and to track the progress of remediation. Cisco Security IntelliShield Alert Manager Service delivers the intelligence that agency IT security groups need for effective threat protection. Staff members use the customizable, Web-based threat and vulnerability alert service to quickly access timely, accurate, and credible information about vulnerabilities that might affect their environments—without time-consuming research. IT security staff can spend less time looking through mailing lists and vendor Websites for new security threats, and more time on remediation and proactive protection. For more information, visit [www.cisco.com/go/intellishield](http://www.cisco.com/go/intellishield)

### **Cisco Video Surveillance**

Federal government agencies rely on surveillance video for applications as diverse as border security and building security. But video feeds from traditional analog systems can only be accessed from certain terminals, over dedicated video networks, and cannot easily be integrated with other building management systems and sensors to provide actionable information. Cisco Video Surveillance systems take advantage of the agency's IP network for video transmission, monitoring, recording, and management. One advantage is that authorized personnel can access video from any Web browser, enabling real-time incident response, investigation, and resolution. Another is that video can be integrated with input from other sensors connected to the IP network, such as motion detectors. With the Cisco Video Surveillance solution, agencies can continue to use their existing analog video cameras and other devices, extending the life of their investments while increasing their value. For more information, visit [www.cisco.com/go/videosurveillance](http://www.cisco.com/go/videosurveillance)

## Cisco Network Admission Control Appliance

Cisco Network Admission Control (NAC) Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control product. The Cisco NAC product uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With Cisco NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network. If the device complies and the employee is authorized, network access is granted. If the device is noncompliant, the Cisco NAC Appliance quarantines the device and performs automatic remediation before granting access. For more information, visit [www.cisco.com/go/nac](http://www.cisco.com/go/nac)

## Cisco Security Monitoring, Analysis, and Response System

An essential part of the SISA, Cisco Security Monitoring, Analysis, and Response System (MARS) is an appliance-based solution that agency IT groups can use to quickly identify, understand, manage, and eliminate network attacks. Cisco Security MARS acts as a central repository for all security information and events, collecting and correlating information from firewalls, virtual private networks, intrusion-prevention systems, and hosts from Cisco and other vendors. Rather than trying to make sense of thousands of daily security events from different devices in the network, agency IT groups can consult one source, Cisco Security MARS, to view relevant, actionable information that has already been aggregated and consolidated. Comprehensive reporting reduces the amount of time needed for federal regulatory compliance. Cisco Security MARS also enables rapid threat detection and mitigation by pinpointing the source of an attack. For more information, visit [www.cisco.com/go/mars](http://www.cisco.com/go/mars)

## Cisco Adaptive Security Appliance

The Cisco ASA 5500 Series Adaptive Security Appliance is a modular platform that provides the next generation of security and VPN services. It combines multiple security functions that federal agencies need for secure information sharing with their own employees and others in the community of interest. Providing security functions in one chassis reduces operational expense and simplifies government data centers. Available modules, called Cisco ASA Editions, include firewall, intrusion prevention, anti-x, and VPN. For more information, visit [www.cisco.com/go/asa](http://www.cisco.com/go/asa)



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

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](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARtNet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered 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. (0711R)