



Corporate
Alliance



SOLUTIONS

IBM and Cisco deliver Automated End Point Security Compliance and Remediation

IBM and Cisco: Next Generation e-business Solutions

Highlights:

- **Links IBM and Cisco products to help cost-effectively improve efficiency in managing network access security policy and end point security compliance**
- **Helps to enforce consistent security policy and compliance to these security policies across the entire network by combining centralized policy management with automated business processes**
- **Automates the security scans of end points accessing the network and the remediation of end points determined to be noncompliant**
- **Helps eliminate errors associated with manual security checks**
- **Can greatly reduce the time required to provide users with access to network resources and applications**
- **Collects and analyzes security status data to facilitate quick response to internal audits and regulatory mandates**

Threats to the Enterprise

To address the challenges of competing in an on demand world, organizations are leveraging their IT infrastructures and extending the use of their IT investments in networks, systems, and applications to efficiently connect with customers, suppliers, and business partners. However, while many-to-many connectivity can drive immense benefits, it also can yield corresponding risks. The recent spate of viruses, worms, and Internet attacks caused significant IT infrastructure damage and a massive loss of productivity within many enterprises. Businesses typically spend more to combat these evolving threats, yet their security capabilities often have not risen to meet the need.

IBM and Cisco Systems are helping enterprises address these security exposures in two key areas. The first is managing the identities of users who connect to the enterprise and the second is dealing with the “wellness” of a device connecting to the network. By knowing the identity of the individual connecting to the corporate network, an enterprise can better control the user’s access. The IBM Integrated Security Solution for Cisco Networks identifies the available IBM products and services offerings that contribute to addressing these security concerns on Cisco networks. This solution brief will address techniques and identify the relevant components available from Cisco and the IBM Integrated Security Solution for Cisco Networks that address the “wellness” of a device connecting to the network.

Integrated end point security compliance

increase the security of your network

Automated End Point Security Compliance as a Competitive Advantage

The increasing number of end points—laptops, desktops, and servers, all running different software—used to access a network can greatly impact the security of the enterprise. End points that connect to the enterprise and are corrupted in some way can infect other parts of the enterprise and cause significant IT infrastructure damage and loss of productivity. Additionally, organizations need to address security compliance as they are faced with an increasing number of internal, industry, and government policies, standards, and regulations.

The growing number and types of end points the enterprise needs to manage frequently forces businesses to spend more to control electronic threats, yet conventional solutions often do not meet this challenge. Traditionally, IT administrators manually manage end point devices for security compliance. This management process can be error-prone, time- and labor-intensive, and generally cannot be implemented consistently or cost effectively. The advantages of a policy-based security solution that automates the detection of vulnerabilities in end points and then isolates and remedies noncompliant end points can include the following:

- The administrative cost of manually monitoring and remediating end points can be reduced
- Automatic monitoring and remediating end points can prevent IT infrastructure damage
- Establishment, management, and automation of the execution of security policies can be done efficiently
- Delays in network access that can negatively impact a user's ability or willingness to do business can be reduced
- Reporting—Quickly produce rich reports in response to internal audits and regulatory mandates

Leverage IBM and Cisco Products to Attain a Policy-Based Security Infrastructure

Enterprises need to efficiently and effectively monitor end points for security compliance to security policies, isolate end points from the secure network, remedy noncompliant end points, manage security policies, and satisfy audits. IBM and Cisco Systems have collaborated to help organizations' IT systems support their enterprises' security needs with great efficiency and agility. IBM and Cisco have collaborated to offer customers a policy-based security compliance and remediation alternative. The results of this collaboration help enterprises implement the end point and security policy management they need to mitigate weaknesses in their organizations' internal security controls and optimize security compliance with regulations and audits.

The IBM Tivoli Security Compliance Manager has been enhanced to integrate with the Cisco Trust Agent. Cisco's Network Admission Control program (Cisco NAC) is a Cisco-led, multi-partner program designed to limit damage caused by viruses and worms. In a Cisco NAC-enabled infrastructure, Cisco Trust Agent and Cisco Secure Access Control Server (Cisco Secure ACS) are integral parts of the end point security compliance and remediation processes managed autonomically by IBM Tivoli Security Compliance Manager and IBM Tivoli Provisioning Manager. Cisco Trust Agent, in conjunction with Cisco Secure ACS, grants network access only to end points compliant with security policies defined by Tivoli Security Compliance Manager.

These integrated IBM and Cisco products can help to protect network enterprises from end points that may be corrupted, reduce end point and policy management cost and time, and drive security compliance across the enterprise network.

A Policy-Based Security Solution Provides Multiple Benefits

The IBM Integrated Security Solution for Cisco Networks offers a security-rich, policy-based security compliance and remediation solution for small, medium, and large businesses. It can help increase productivity by allowing administrators to focus on revenue-enhancing initiatives. Administrative tasks can be simplified through

- Centralizing administration of defined security policy
- Automating security policy enforcement and execution
- Automating end point security scans
- Notification of security compliance vulnerabilities before a potential security incident occurs
- Generating status reports for rapid response to internal, industry, and government audits
- Embedding provisioning engine that remedies noncompliant end points

By knowing the security compliance state of each end point connecting to the network, an enterprise can control the relationship of the end point to the network by denying or restricting access if the end point does not conform to policy using Cisco NAC. Many end points, such as those of vendors, may be legitimate but should be granted only limited network access. Rogue devices—devices outside the controls of the enterprise—can masquerade as other users or identities with impunity and pose a substantial risk.

IBM Tivoli Security Compliance Manager helps enterprises define, maintain, and enforce consistent security policies. The software comes with pre-defined, recommended security policies that can be customized to fit specific corporate, industry, or regulatory security policies. It acts as an early warning system by identifying security vulnerabilities and security policy violations so an enterprise can address and correct security compliance issues prior to costly damage being incurred. It collects and audits data about security status, and allows administrators to quickly produce detailed reports to help comply with regulations and audits. Tivoli Security Compliance Manager automates security scans of servers and desktop systems, both before and during end point connections to the network. The software triggers the remediation subsystem so that noncompliant devices can be isolated and repaired.

By centralizing and automating security policy and security compliance management tasks, Tivoli Security Compliance Manager can help to reduce the time and cost associated with manual management tasks, reduce human error, and improve business operations and efficiencies.

management can help to and productivity of your administrators and end users.

IBM Tivoli Provisioning Manager automates manual tasks of provisioning and configuring servers, operating systems, middleware, applications, storage, and network devices. The software uses workflows to provide control and configuration of major vendors' products. It allows an enterprise to centrally manage and automate the software and configuration for end points. Tivoli Provisioning Manager automates the remediation of noncompliant end points by installing required software updates or by correcting configuration issues. The remediation capabilities of Tivoli Provisioning Manager include software levels—typically operating system levels and fix packs; patch levels; virus and firewall update; last virus scan; password strength and history; and policy level. Tivoli Provisioning Manager runs a set of processes to determine what needs to be corrected on the noncompliant end point, and then triggers automated processes to make the required corrections. An enterprise can customize the remediation capabilities of Tivoli Provisioning Manager to include the specific updates that it requires of its end points.

Through workflows and automation, Tivoli Provisioning Manager provides self-managing end point remediation, through patches or configuration corrections. This can help an enterprise to reduce the time, cost, and errors associated with manual remediation tasks by centrally managing and automating the remediation processes for noncompliant end points. It works with an enterprise's existing IT infrastructure to provide optimal resource provisioning.

Integrated Security Compliance and Remediation Components

Cisco elements to address integrated security compliance and remediation include Cisco Trust Agent and Cisco Secure ACS. IBM elements include IBM Tivoli Security Compliance Manager, IBM Tivoli Provisioning Manager, and in the Microsoft Windows environment IBM ThinkPad and ThinkCentre systems that include the ThinkVantage technology Rescue and Recovery with Antidote Delivery Manager.

IBM Tivoli Security Compliance Manager is a policy-based software solution that works across legacy and on demand operating environments. It allows enterprises to centralize security policy definitions and automate the scanning of systems for security compliance. In a Cisco NAC-enabled infrastructure, Tivoli Security Compliance Manager triggers a set of processes to move a noncompliant end point to an isolated virtual local area network (VLAN) with limited or no network access. Tivoli Security Compliance Manager enables businesses to realize lower costs, higher levels of security, and a rapid return on investment. Centralization and automation provide consistent security compliance across the entire organization and can help enterprises operate more efficiently and reduce costs through:

- Automating the enforcement and execution of security policies
- Automating security scans of servers and desktop systems
- Helping identify software security vulnerabilities prior to costly damage being inflicted by security incidents
- Addressing security compliance issues in regulations and standards by automating security compliance tasks, monitoring correspondence, and reducing human error

- Providing consistent security auditing across the entire organization
- Collecting and analyzing security data to quickly produce detailed reports for audits

IBM Tivoli Provisioning Manager provides a set of software management capabilities that enterprises can leverage to centrally manage and automate the remediation and software management processes for noncompliant end points. Tivoli Security Compliance Manager sends Tivoli Provisioning Manager a token that represents the reason for the quarantine of a noncompliant end point. Tivoli Provisioning Manager interrogates the token to understand the reason, and runs a set of processes to trigger the remediation of the end point through a software distribution, configuration or patch management capability like Secure SHell or Tivoli Configuration Manager, either by installing software updates or by correcting configuration issues. Through workflows, Tivoli Provisioning Manager automates manual provisioning and deployment processes. Enterprises can create customized workflows to implement their company's best practices and procedures. These procedures can then be automated and executed in a consistent, error-free manner.

IBM Rescue and Recovery with Antidote Delivery Manager, available with IBM ThinkPad and ThinkCentre systems, provides capabilities similar to Tivoli Provisioning Manager and Secure SHell for the Microsoft® Windows® environment. Antidote Delivery Manager enables noncompliant Windows end points to retrieve updates and become compliant. It uses Cisco NAC to isolate a noncompliant Windows end point from the secure network. When the noncompliant end point is isolated, Antidote Delivery Manager automatically checks a repository for required updates and enables the end point to retrieve the updates it needs to become compliant. In environments where Tivoli software is not present, Antidote Delivery Manager can also address situations in which the latest Antidote Delivery Manager log entry does not match the requirements for the enterprise.

Cisco Trust Agent is a core component of Cisco NAC. Cisco Trust Agent software is installed on hosts whose security policy status needs to be validated before the network permits access. It is integrated with Cisco Security Agent—software that provides threat protection for servers and desktop systems. Cisco Trust Agent allows Cisco NAC to determine if Cisco Security Agent or antivirus software is installed and current, and also determines current operating system and patch levels. Cisco Trust Agent is available at no charge—either as a standalone application or bundled with Cisco Security Agent.

Cisco Secure ACS is a centralized identity networking solution that manages user and administrative access to the network. Cisco Secure ACS is a highly scalable, high-performance access control server that enforces security policy by allowing network administrators to control the access rights of users. It extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework. Cisco Secure ACS maximizes flexibility and mobility and increases security and end user productivity.

Solution Components:

Cisco Products

Cisco Trust Agent
Cisco Secure Access Control Server

Core IBM Products from the IBM Integrated Security Solution for Cisco Networks

IBM Tivoli Security Compliance Manager
IBM Tivoli Provisioning Manager
IBM ThinkPad or ThinkCentre systems that include Rescue and Recovery with Antidote Delivery Manager

Solution can also be complemented by:

IBM Tivoli Identity Manager
IBM Tivoli Access Manager for e-business
IBM 

World-Class Services to Reduce Security Risks

One of the world's leading services providers, IBM Global Services is Cisco's largest provider of services. IBM Global Services brings experienced skills in IT, networking, security, and infrastructure to implement a security-enhanced enterprise project. These capabilities of delivering worldwide Cisco solutions for customers have been honed through years of consulting for and deploying user installation solutions of all sizes.

IBM Global Services has developed technical and process skills with the technologies associated with security from Cisco networking, security compliance, and client security concerns. This experience can be applied to help meet the risk tolerance associated with an IT infrastructure so that an organization can meet its goals, protect its assets, and manage security.

From consulting, planning, and design through integration and testing, IBM Global Services can offer end-to-end security services solutions. IBM Global Services business and technology consultants, with extensive industry experience and proven track record, understand the key role that IT security plays in a business.

For more information on how IBM and Cisco team together to provide end point and security policy compliance management, see:

www.cisco.com/go/ibm
www.ibm.com/services/alliances/cisco
www.ibm.com/tivoli
www.ibm.com/security
www.ibm.com/software



Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
www.cisco.com/go/ibm



IBM Corporation
Route 100
Somers, NY 10589
www.ibm.com/security/cisco

Copyright © 2004 IBM Corporation. All rights reserved.

IBM, the IBM logo, the e-business logo, the On Demand Business logo, the eServer logo, Tivoli, ThinkPad, and ThinkCentre are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates or for an unlimited period of time. IBM reserves the right to alter product offerings, prices, and specifications at any time, without notice.

Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.